ETSI TS 129 228 V9.6.0 (2011-06)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
IP Multimedia (IM) Subsystem Cx and Dx Interfaces;
Signalling flows and message contents
(3GPP TS 29.228 version 9.6.0 Release 9)



Reference
RTS/TSGC-0429228v960

Keywords
GSM, LTE, UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Intellectual Property Rights 2
Foreword 2
Foreword 6
1 Scope 7
2 References 7
3 Definitions, symbols and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 8
4 Main Concept 9
5 General Architecture 9
5.1 Functional requirements of network entities 9
5.1.1 Functional requirements of P-CSCF 9
5.1.2 Functional requirements of I-CSCF 9
5.1.3 Functional requirements of S-CSCF 9
5.1.4 Functional requirements of HSS 9
5.1.5 Functional classification of Cx interface procedures 9
5.1.6 Functional Requirements of the Presentity Presence Proxy 10
6 Procedure Descriptions 10
6.1 Location management procedures 11
6.1.1 User registration status query 11
6.1.1.1 Detailed behaviour 12
6.1.2 S-CSCF registration/deregistration notification 14
6.1.2.1 Detailed behaviour 18
6.1.3 Network initiated de-registration by the HSS, administrative 22
6.1.3.1 Detailed behaviour 23
6.1.4 User location query 24
6.1.4.1 Detailed behaviour 25
6.2 User data handling procedures 26
6.2.1 User Profile download 26
6.2.2 HSS initiated update of User Profile 27
6.2.2.1 Detailed behaviour 27
6.3 Authentication procedures 28
6.3.1 Detailed behaviour 32
6.4 User identity to HSS resolution 33
6.5 Implicit registration 34
6.5.1 S-CSCF initiated procedures 34
6.5.1.1 Registration 34
6.5.1.2 De-registration 34
6.5.1.3 Authentication 34
6.5.1.4 Downloading the user profile 34
6.5.1.5 Initiation of a session to a non-registered user 35
6.5.2 HSS initiated procedures 35
6.5.2.1 Update of User Profile 35
6.5.2.2 De-registration 35
6.5.2.3 Update of the Charging information 35
6.6 Download of the Relevant User Profile 35
6.6.1 HSS initiated update of User Profile 36
6.6.2 S-CSCF operation 36
6.7 S-CSCF Assignment 36
7 Information element contents 38
7.1 Visited Network Identifier 38

7.2 Public User Identity 38
7.2a Public Service Identity 38
7.2b Wildcarded Public Identity 38
7.2c Void 38
7.3 Private User Identity 38
7.3a Private Service Identity 38
7.4 S-CSCF Name 38
7.4a AS Name 38
7.5 S-CSCF Capabilities 39
7.6 Result 39
7.7 User Profile 39
7.8 Server Assignment Type 39
7.9 Authentication Data 39
7.9.1 Item Number 39
7.9.2 Authentication Scheme 39
7.9.3 Authentication Information 39
7.9.4 Authorization Information 39
7.9.5 Confidentiality Key 39
7.9.6 Integrity Key 39
7.9.7 Authentication Context 40
7.9.8 Digest Authenticate 40
7.9.8.1 Digest Realm 40
7.9.8.2 Void 40
7.9.8.3 Digest Algorithm 40
7.9.8.4 Digest QoP 40
7.9.8.5 Digest HA1 40
7.9.9 Line Identifier 40
7.10 Number Authentication Items 40
7.11 Reason for de-registration 40
7.12 Charging information 40
7.13 Routing information 40
7.14 Type of authorization 41
7.15 Void 41
7.16 User Data Already Available 41
7.17 Associated Private Identities 41
7.18 Originating-Request 41
7.19 User Authorization Request Flags 41
7.20 Loose-Route Indication 41
7.21 S-CSCF Restoration Information 41
7.22 Associated Registered Private Identities 41
7.23 Multiple Registration Indication 41
7.24 Session-Priority 42
7.25 Identities with Emergency Registration 42

8 Error handling procedures 42
8.1 Registration error cases 42
8.1.1 Cancellation of the old S-CSCF 42
8.1.2 Error in S-CSCF name 42
8.1.3 Error in S-CSCF assignment type 43

9 Protocol version identification 43

10 Operational Aspects 43

Annex A (normative): Mapping of Cx operations and terminology to Diameter 44

A.1 Introduction 44

A.2 Cx message to Diameter command mapping 44

A.3 Cx message parameters to Diameter AVP mapping 44

A.4 Message flows 45
A.4.1 Registration– user not registered 46

A.4.2 Registration – user currently registered 47
A.4.3 UE initiated de-registration 47
A.4.4 Network initiated de-registration 48
A.4.4.1 Registration timeout 48
A.4.4.2 Administrative de-registration 48
A.4.4.3 De-registration initiated by service platform 49
A.4.5 UE Terminating SIP session set-up 49
A.4.6 Initiation of a session to a non-registered user 50
A.4.6a AS originating session on behalf of a non-registered user 50
A.4.7 User Profile update 51

Annex B (informative): User profile UML model 52

B.1 General description 52

B.2 Service profile 52
B.2.1 Public Identification 53
B.2.1A Core Network Service Authorization 54
B.2.2 Initial Filter Criteria 54
B.2.3 Service Point Trigger 56

Annex C (informative): Conjunctive and Disjunctive Normal Form 58

Annex D (informative): High-level format for the User Profile 61

Annex E (normative): XML schema for the Cx interface user profile 62

Annex F (normative): Definition of parameters for service point trigger matching 66

Annex G (informative): Change history 67

History 71

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
 - 1 presented to TSG for information;
 - 2 presented to TSG for approval;
 - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This 3GPP Technical Specification (TS) specifies:

1. The interactions between the HSS (Home Subscriber Server) and the CSCF (Call Session Control Functions), referred to as the Cx interface.

2. The interactions between the CSCF and the SLF (Server Locator Function), referred to as the Dx interface.

The IP Multimedia (IM) Subsystem stage 2 is specified in 3GPP TS 23.228 [1] and the signalling flows for the IP multimedia call control based on SIP and SDP are specified in 3GPP TS 24.228 [2].

This document addresses the signalling flows for Cx and Dx interfaces.

This document also addresses how the functionality of Px interface is accomplished.

The Presence Service Stage 2 description (architecture and functional solution) is specified in 3GPP TS 23.141 [10].

2 References

[1] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2"

[2] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP"

[3] 3GPP TS 33.203: "Access security for IP-based services"

[4] 3GPP TS 23.002: "Network architecture"

[5] 3GPP TS 29.229: "Cx Interface based on Diameter – Protocol details"

[6] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IP Multimedia (IM) call model"

[7] IETF RFC 2045 "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies"

[8] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on SIP and SDP" – stage 3

[9] IETF RFC 3588 "Diameter Base Protocol"

[10] 3GPP TS 23.141: "Presence Service; Architecture and Functional Description"

[11] IETF RFC 3261 "SIP: Session Initiation Protocol"

[12] IETF RFC 4566 "SDP: Session Description Protocol"

[13] IEEE 1003.1-2004, Part 1: Base Definitions

[14] IETF RFC 2486 "The Network Access Identifier"

[15] IETF RFC 3966 "The tel URI for Telephone Numbers"

[16] IETF RFC 2617 "HTTP Authentication: Basic and Digest Access Authentication"

[17] 3GPP TS 23.003: "Numbering, addressing and identification"

[18] 3GPP TS 23.008: "Organization of subscriber data"

[19] 3GPP TS 23.380: "IMS Restoration Procedures"

[20] IETF draft-dawes-sipping-debug-02 (August 2010): "Private Extension to the Session Initiation Protocol (SIP) for Debugging".

[21] IETF RFC 4005: "Diameter Network Access Server Application"

[22] IETF RFC 4412: "Communications Resource Priority for the Session Initiation Protocol (SIP)"

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Common Part (of a user profile): Contains Initial Filter Criteria instances that should be evaluated both for registered and unregistered Public User Identities, or for unregistered Public Service Identities in the S-CSCF.

Complete user profile: Contains the Initial Filter Criteria instances of all three different user profile parts; registered part, unregistered part and common part.

Distinct Public Service Identity: An individual Public Service Identity that is stored in the HSS as such.

IP Multimedia session: IP Multimedia session and IP Multimedia call are treated as equivalent in this specification.

Authentication pending flag: A flag that indicates that the authentication of a Public User Identity - Private User Identity pair is pending and waiting for confirmation.

Charging information: Data that is sent in the Charging-Information AVP.

Implicitly registered Public User Identity set: A set of Public User Identities, which are registered and de-registered simultaneously when any of the Public User Identities belonging to that set is registered or de-registered.

Not Registered State: Public Identity is not Registered and has no S-CSCF assigned.

Private Identity: Either a Private User Identity or a Private Service Identity.

Public Identity: Either a Public User Identity or a Public Service Identity.

Registered Part (of a user profile): Contains Initial Filter Criteria instances that should be evaluated only for registered Public User Identities in the S-CSCF. iFCs from the registered part need not be evaluated when the Public Identity is unregistered.

Registered State: Public User Identity is Registered at the request of the user and has an S-CSCF assigned.

S-CSCF reassignment pending flag: A flag that is handled only when IMS Restoration Procedures are supported.and that indicates that the subscription may be reassigned to a new S-CSCF (i.e. the current S-CSCF is not responding)

Unregistered part (of a user profile): Contains Initial Filter Criteria instances that should be evaluated only for unregistered Public Identities in the S-CSCF. iFCs from the unregistered part need not be evaluated when the Public User Identity is registered.

Unregistered State: Public Identity is not Registered but has a serving S-CSCF assigned to execute Unregistered state services as a consequence of a terminating request, or an originating request from an AS on behalf of a user, or there is an S-CSCF keeping the user profile stored.

User information: The user related data that the S-CSCF requests from the HSS or HSS pushes to the S-CSCF, e.g. user profile and charging information.

User profile: Data that is sent in the User-Data AVP.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AVP	Attribute Value Pair
C	Conditional
CSCF	Call Session Control Function
GIBA	GPRS-IMS-Bundled-Authentication

HSS	Home Subscriber Server
IE	Information Element
IP	Internet Protocol
I-CSCF	Interrogating CSCF
IM	IP Multimedia
IMS	IP Multimedia Subsystem
M	Mandatory
NASS	Network Attachment SubSystem
O	Optional
P-CSCF	Proxy CSCF
SIP	Session Initiation Protocol
SLF	Server Locator Function
S-CSCF	Serving CSCF

4 Main Concept

This document presents the Cx interface related functional requirements of the communicating entities.

It gives a functional classification of the procedures and describes the procedures and message parameters.

Error handling flows, protocol version identification, etc. procedures are also included.

5 General Architecture

This clause further specifies the architectural assumptions associated with the Cx reference point, building on 3GPP TS 23.228 [1] and also the Px reference point building upon 3GPP TS 23.141 [10].

5.1 Functional requirements of network entities

5.1.1 Functional requirements of P-CSCF

There is no requirement for the interaction between the P-CSCF and the HSS.

5.1.2 Functional requirements of I-CSCF

The I-CSCF communicates with the HSS over the Cx interface.

For functionality of the I-CSCF refer to 3GPP TS 23.002 [4].

5.1.3 Functional requirements of S-CSCF

The S-CSCF communicates with the HSS over the Cx interface.

For functionality of the S-CSCF refer to 3GPP TS 23.002 [4].

5.1.4 Functional requirements of HSS

The HSS communicates with the I-CSCF and the S-CSCF over the Cx interface.

For functionality of the HSS refer to 3GPP TS 23.002 [4].

5.1.5 Functional classification of Cx interface procedures

Operations on the Cx interface are classified in functional groups:

1. Location management procedures

- The operations regarding registration and de-registration.
- Location retrieval operation.

2. User data handling procedures
 - The download of user information during registration and to support recovery mechanisms.
 - Operations to support the updating of user data and recovery mechanisms.
3. User authentication procedures
4. IMS Restoration Procedures (see 3GPP TS 23.380 [19]) to support S-CSCF service interruption

5.1.6 Functional Requirements of the Presentity Presence Proxy

The interaction between the Presentity Presence Proxy and the HSS, referred to as the Px interface, is handled using the mechanisms defined for the Cx interface.

6 Procedure Descriptions

In the tables that describe the Information Elements transported by each command, each Information Element is marked as (M) Mandatory, (C) Conditional or (O) Optional in the Category "Cat." column. The application level specification overrides the ABNF defining the presence of the AVPs to be included in the Diameter commands. The category defined by the Information Element table shall always be the same, i.e. Optional; or more restrictive, i.e. Mandatory or Conditional, than the presence requirements defined by the ABNF syntax, e.g. a required AVP in the ABNF shall not be overridden by an Optional IE but an Optional AVP in the ABNF may be overridden by the Mandatory or Conditional IE Category.

- A mandatory Information Element shall always be present in the command. If this Information Element is absent, an application error occurs at the receiver and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.
- A conditional Information Element (marked as (C) in the table) shall be present in the command if certain conditions are fulfilled.
 - If the receiver detects that those conditions are fulfilled and the Information Element is absent, an application error occurs and an answer message shall be sent back to the originator of the request with the Result-Code set to DIAMETER_MISSING_AVP. This message shall also include a Failed-AVP AVP containing the missing Information Element i.e. the corresponding Diameter AVP defined by the AVP Code and the other fields set as expected for this Information Element.
 - If those conditions are not fulfilled, the Information Element shall be absent. If however this Information Element appears in the message, it shall not cause an application error and it may be ignored by the receiver if this is not explicitly defined as an error case. Otherwise, an application error occurs at the receiver and an answer message with the Result-Code set to DIAMETER_AVP_NOT_ALLOWED shall be sent back to the originator of the request. A Failed-AVP AVP containing a copy of the corresponding Diameter AVP shall be included in this message.
- An optional Information Element (marked as (O) in the table) may be present or absent in the command, at the discretion of the application at the sending entity. Absence or presence of this Information Element shall not cause an application error and may be ignored by the receiver.

When a procedure is required to determine whether two S-CSCF names are equal, the rules for SIP URI comparison specified in RFC 3261 chapter 19.1.4 shall apply.

When a procedure is required to determine the Public Identity used for an identity lookup in HSS and SLF, the HSS and SLF shall derive the Public Identity from the SIP URI or Tel URI contained in the Public-Identity AVP, if not already in canonical form as per 3GPP TS 23.003 [17], as described below:

- If the Public-Identity AVP contains a SIP URI, the HSS and SLF shall follow rules for conversion of SIP URI into canonical form as specified in IETF RFC 3261 [11] chapter 10.3.

- If the Public-Identity AVP contains a Tel URI in E.164 format, the HSS and SLF shall remove visual separators and remove all URI parameters.

Unknown permanent failure error codes shall be treated in the same way as DIAMETER_UNABLE_TO_COMPLY. For unknown transient failure error codes the request may be repeated, or handled in the same way as DIAMETER_UNABLE_TO_COMPLY.

6.1 Location management procedures

6.1.1 User registration status query

This procedure is used between the I-CSCF and the HSS during SIP registrations. The procedure is invoked by the I-CSCF, corresponds to the combination of the functional level operations Cx-Query and Cx-Select-Pull (see 3GPP TS 23.228 [1]) and is used:

- To authorize the registration of the distinct Public User Identity, checking multimedia subsystem access permissions and roaming agreements.

- To perform a first security check, determining whether the distinct Public User Identity in the message is associated with the Private User Identity sent in the message.

- To obtain either the S-CSCF where the distinct Public User Identity is registered or unregistered (i.e. registered as a consequence of an originating or terminating request or there is a S-CSCF keeping the user profile stored), or the list of capabilities that the S-CSCF has to support.

This procedure is mapped to the commands User-Authorization-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.1.1.1 and 6.1.1.2 detail the involved information elements.

Table 6.1.1.1: User registration status query

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity (See 7.2)	Public-Identity	M	Public User Identity to be registered
Visited Network Identifier (See 7.1)	Visited-Network-Identifier	M	Identifier that allows the home network to identify the visited network
Type of Authorization (See 7.14)	User-Authorization-Type	C	Type of authorization requested by the I-CSCF. If the request corresponds to a de-registration, i.e. Expires field or expires parameter in Contact field in the REGISTER method is equal to zero, this AVP shall be present in the command and the value shall be set to DE-REGISTRATION. If the request corresponds to an initial registration or a re-registration, i.e. Expires field or expires parameter in Contact field in the REGISTER method is not equal to zero then this AVP may be absent from the command. If present its value shall be set to REGISTRATION. If the request corresponds to an initial registration or a re-registration and the I-CSCF explicitly queries the S-CSCF capabilities, then this AVP shall be present in the command and the value shall be set to REGISTRATION_AND_CAPABILITIES. The I-CSCF shall use this value when the S-CSCF currently assigned to the Public User Identity in the HSS, cannot be contacted and a new S-CSCF needs to be selected.
Private User Identity (See 7.3)	User-Name	M	Private User Identity
Routing Information (See 7.13)	Destination-Host, Destination-Realm	C	If the I-CSCF knows HSS name Destination-Host AVP shall be present in the command. Otherwise, only Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the I-CSCF.
UAR Flags (See 7.19)	UAR-Flags	O	This Information Element contains a set of indications. See 7.19 for the content of the information element.

Table 6.1.1.2: User registration status response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
S-CSCF capabilities (See 7.5)	Server-Capabilities	O	Required capabilities of the S-CSCF to be assigned to the IMS Subscription.
S-CSCF Name (See 7.4)	Server-Name	C	Name of the assigned S-CSCF.

6.1.1.1 Detailed behaviour

The HSS shall, in the following order (if there is an error in any of the following steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.229 [5]):

1. Check that the Private User Identity and the Public User Identity exists in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check that the Public User Identity matches a distinct Public User Identity in the HSS. If it doesn't, the Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

3. Check that the Public User Identity received in the request is associated with the Private User Identity received in the request. If not Experimental-Result-Code shall be set to DIAMETER_ERROR _IDENTITIES_DONT_MATCH.

4. Check whether the Public User Identity received in the request is barred from the establishment of multimedia sessions.

 - If it is an IMS Emergency Registration (by checking the UAR Flags) or the Public User Identity received in the request is not barred, continue to step 5.

 - Otherwise, the HSS shall check whether there are other non-barred Public User Identities to be implicitly registered with that one.

 - If so, continue to step 5.

 - If not, Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED.

5. Check the User-Authorization-Type received in the request:

 - If it is REGISTRATION or if User-Authorization-Type is absent from the request, the HSS shall check whether the UAR Flags indicate that this is an IMS Emergency Registration:

 - If it is not, and the Public User Identity is allowed to roam in the visited network (if not Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED) then continue to step 6.

 - If it is an IMS Emergency Registration, authorization shall be granted and the HSS shall not perform any check regarding roaming. Continue to step 6.

 - If it is DE_REGISTRATION, the HSS may not perform any check regarding roaming. Continue to step 6.

 - If it is REGISTRATION_AND_CAPABILITIES, the HSS shall check whether the UAR Flags indicate that this is an IMS Emergency Registration:

 - If it is not, and the Public User Identity is allowed to roam in the visited network (if not Experimental-Result-Code shall be set to DIAMETER_ERROR _ROAMING_NOT_ALLOWED) and authorized to register (if not Result-Code shall be set to DIAMETER_AUTHORIZATION_REJECTED). The HSS shall return the Server-Capabilities AVP, which enables the I-CSCF to select an S-CSCF. If an S-CSCF is already assigned in the HSS and IMS Restoration Procedures are supported in the HSS, the HSS shall set the S-CSCF reassignment pending flag and shall allow overwriting of the S-CSCF name in the next SAR request. The returned capabilities must satisfy all the requirements of all the service profiles associated with the IMS Subscription. The Server-Capabilities AVP may be absent, to indicate to the I-CSCF that it can select any available S-CSCF. Result-Code shall be set to DIAMETER_SUCCESS. The HSS shall not return any S-CSCF name. Stop processing.

 - If it is an IMS Emergency Registration, authorization shall be granted and the HSS shall not perform any check regarding roaming. The HSS shall return the Server-Capabilities AVP, which enables the I-CSCF to select an S-CSCF. The returned capabilities must satisfy all the requirements of all the service profiles associated with the IMS Subscription. The Server-Capabilities AVP may be absent, to indicate to the I-CSCF that it can select any available S-CSCF. Result-Code shall be set to DIAMETER_SUCCESS. The HSS shall not return any S-CSCF name. Stop processing.

6. Check the state of the Public User Identity received in the request:

 - If it is registered, the HSS shall return the stored S-CSCF name. No S-CSCF capabilities shall be present in the response. If User-Authorization-Type is equal to REGISTRATION or is absent, Experimental-Result-Code shall be set to DIAMETER_SUBSEQUENT_REGISTRATION. If User-Authorization-Type is equal to DE-REGISTRATION, Result-Code shall be set to DIAMETER_SUCCESS.

 - If it is unregistered (i.e. registered as a consequence of an originating or terminating request or there is an S-CSCF keeping the user profile stored) and User-Authorization-Type is equal to DE-REGISTRATION, the HSS shall return the stored S-CSCF name and the Result-Code shall be set to DIAMETER_SUCCESS. If the User-Authorization-Type is equal to REGISTRATION or is absent, then the HSS shall return the stored S-

CSCF name and the Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.

- If it is not registered yet, the HSS shall check the value of User-Authorization-Type received in the request:
 - If the value of User-Authorization-Type is DE_REGISTRATION and the Authentication pending flag is set, the HSS shall return the stored S-CSCF name and Experimental-Result-Code set to DIAMETER_SUCCESS. The HSS shall not return any S-CSCF capabilities. Otherwise, if Authentication pending flag is not set, the HSS shall not return any S-CSCF name or S-CSCF capabilities. The HSS shall set the Experimental-Result-Code to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED in the response.
 - If the value of User-Authorization-Type is REGISTRATION or is absent, then the HSS shall check if there is at least one Public User Identity within the IMS Subscription with an S-CSCF name assigned.
 - If there is at least one Public User Identity within the IMS Subscription that is registered, the HSS shall return the S-CSCF name assigned for that Public User Identity and Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
 - If there is at least one Public User Identity within the IMS Subscription that is unregistered (i.e registered as a consequence of an originating or terminating request or there is an S-CSCF keeping the user profile stored), then the HSS shall return the stored S-CSCF name and the Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
 - If there is no identity of the user within the same IMS Subscription that is registered or unregistered, the HSS shall check if there is an S-CSCF name stored for the user (e.g. the user is being authenticated by the S-CSCF as indicated by the Authentication pending flag). If it is, the HSS shall return the stored S-CSCF name and Experimental-Result-Code set to DIAMETER_SUBSEQUENT_REGISTRATION. The HSS shall not return any S-CSCF capabilities.
 - If there is not any Public User Identity within the IMS Subscription with an S-CSCF name assigned, then the HSS shall return the Server-Capabilities AVP, which enables the I-CSCF to select an S-CSCF. The returned capabilities shall satisfy all the requirements of all the service profiles associated with the IMS Subscription. The Server-Capabilities AVP may be absent, to indicate to the I-CSCF that it may select any available S-CSCF. Experimental-Result-Code shall be set to DIAMETER_FIRST_REGISTRATION. The HSS shall not return any S-CSCF name.

If the HSS cannot fulfil received request, e.g. due to database error, it shall set Result-Code to DIAMETER_UNABLE_TO_COMPLY. No S-CSCF name or S-CSCF capabilities shall be present in the response.

6.1.2 S-CSCF registration/deregistration notification

This procedure is used between the S-CSCF and the HSS. The procedure is invoked by the S-CSCF, corresponds to the combination of the operations Cx-Put and Cx-Pull (see 3GPP TS 23.228 [1]) and is used:

- To assign an S-CSCF to a Public Identity, or to clear the name of the S-CSCF assigned to one or more Public Identities.
- To download from HSS the relevant user information for the S-CSCF.
- To backup and retrieve the S-CSCF Restoration Information (see 3GPP TS 23.380 [19]) in the HSS.

This procedure is mapped to the commands Server-Assignment-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.1.2.1 and 6.1.2.2 describe the involved information elements.

Table 6.1.2.1: S-CSCF registration/deregistration notification request

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity / Public Service Identity (See 7.2 and 7.2a)	Public-Identity	C	Public Identity or list of Public Identities. One and only one Public Identity shall be present if the Server-Assignment-Type is any value other than TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION, DEREGISTRATION_TOO_MUCH_DATA, TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME, USER_DEREGISTRATION_STORE_SERVER_NAME or ADMINISTRATIVE_DEREGISTRATION. If Server-Assignment-Type indicates deregistration of some type and Private Identity is not present in the request, at least one Public Identity shall be present.
S-CSCF Name (See 7.4)	Server-Name	M	Name of the S-CSCF.
Private User Identity / Private Service Identity (See 7.3 and 7.3a)	User-Name	C	Private Identity. It shall be present if it is available when the S-CSCF issues the request. It may be absent during the initiation of a session to an unregistered Public Identity. In such situation, Server-Assignment-Type shall contain the value UNREGISTERED_USER. In case of de-registration, Server-Assignment-Type equal to TIMEOUT_DEREGISTRATION, ADMINISTRATIVE_DEREGISTRATION, DEREGISTRATION_TOO_MUCH_DATA or TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME if no Public-Identity AVPs are present then User-Name AVP shall be present.
Server Assignment Type (See 7.8)	Server-Assignment-Type	M	Type of update that the S-CSCF requests in the HSS (e.g: de-registration). See 3GPP TS 29.229 [5] for all the possible values.
User Data Already Available (See 7.16)	User-Data-Already-Available	M	This indicates if the user profile is already available in the S-CSCF. In the case where Server-Assignment-Type is not equal to NO_ASSIGNMENT, REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER, the HSS shall not use User Data Already Available when processing the request.
Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows the HSS name, the Destination-Host AVP shall be present in the command. This information is available if the request belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. This information may not be available if the command is sent as a consequence of a session termination for an unregistered Public Identity. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the S-CSCF.
Wildcarded Public Identity (See 7.2b)	Wildcarded-Public-Identity	O	If the request refers to a Wildcarded PSI or Wildcarded Public User Identity, and the Server-Asignment-Type is set to UNREGISTERED_USER, NO_ASSIGNMENT, TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME, ADMINISTRATIVE_DEREGISTRATION, DEREGISTRATION_TOO_MUCH_DATA or TIMEOUT_DEREGISTRATION, the S-CSCF may include the corresponding Wildcarded PSI or Wildcarded Public User Identity in this information element. If this element is present, it shall be used by the HSS to identify the identity affected by the request. The terms Public Identity or Public Service Identity in the detailed behaviour refer then to the Wildcarded Public Identity.
S-CSCF Restoration Information (See 7.21)	SCSCF-Restoration-Info	C	When the S-CSCF supports IMS Restoration Procedures, if Server-Assignment-Type is REGISTRATION or RE_REGISTRATION, and any of the related restoration information changed compared to the previous one, the S-CSCF shall send this information element to the HSS. This information allows a later retrieval in case of an S-CSCF service interruption.

Multiple-Registration-Indication (See 7.23)	Multiple-Registration-Indication	C	When the S-CSCF supports IMS Restoration Procedures, if Server-Assignment-Type is REGISTRATION and the registration is a multiple registration or an emergency registration, and the Public User Identity is not stored as registered with the Private User Identity as in the request in the S-CSCF, the S-CSCF shall send this information element to the HSS.
Session-Priority (See 7.24)	Session-Priority	O	This information element shall indicate the session's priority to the HSS. If it is not included, the request shall be treated as normal.

Table 6.1.2.2: S-CSCF registration/deregistration notification response

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity / Private Service Identity (See 7.3 and 7.3a)	User-Name	C	Private Identity. It shall be present if it is available when the HSS sends the response. It may be absent in the following error case: when the Server-Assignment-Type of the request is UNREGISTERED_USER and the received Public Identity is not known by the HSS.
Registration result (See 7.6)	Result-Code / Experimental-Result	M	Result of registration. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
User Profile (See 7.7)	User-Data	C	Relevant user profile. It shall be present when Server-Assignment-Type in the request is equal to NO_ASSIGNMENT, REGISTRATION, RE_REGISTRATION or UNREGISTERED_USER according to the rules defined in section 6.6. If the S-CSCF receives more data than it is prepared to accept, it shall perform the de-registration of the Private Identity with Server-Assignment-Type set to DEREGISTRATION_TOO_MUCH_DATA and send back a SIP 3xx or 480 (Temporarily Unavailable) response, which shall trigger the selection of a new S-CSCF by the I-CSCF, as specified in 3GPP TS 24.229 [8].
Charging Information (See 7.12)	Charging-Information	C	Addresses of the charging functions. It shall be present when the User-Data AVP is sent to the S-CSCF. When this parameter is included, either the Primary-Charging-Collection-Function-Name AVP or the Primary-Event-Charging-Function-Name AVP shall be included. All other elements shall be included if they are available.
Associated Private Identities	Associated-Identities	O	This AVP contains all Private Identities, which belong to the same IMS subscription as the Private Identity or Public Identity received in the SAR command. If the IMS subscription contains only single Private Identity this AVP shall not be present.
Loose-Route Indication	Loose-Route-Indication	C	This AVP indicates to the S-CSCF that loose-route mechanism shall be applied to the public identities contained in the user profile received from the HSS. If the loose-route mechanim is required, this AVP shall be present and set to LOOSE_ROUTE_REQUIRED. If the Loose-Route mechanism is not required, this AVP may be either absent or present. If present, it shall be set to LOOSE_ROUTE_NOT_REQUIRED.
S-CSCF Restoration Information (See 7.21)	SCSCF-Restoration-Info	C	This information shall be present if it was stored by the S-CSCF in the HSS and Server-Assignment-Type is either UNREGISTERED_USER or NO_ASSIGNMENT. This information shall also be present if it was stored by the S-CSCF in the HSS and the SAR indicates it is related to a multiple registration and Server-Assignment-Type is REGISTRATION.
Associated Registered Private Identities (See 7.22)	Associated-Registered-Identities	C	This AVP contains all Private Identities that were registered with the Public Identity received in the SAR command. The HSS shall send this information element if the IMS Restoration Procedures are supported and the value of Server-Assignment-Type in the request is REGISTRATION or RE_REGISTRATION and there are other Private Identities different from the Private Identity received in the SAR command being registered with the Public Identity received in the SAR command. Otherwise, this AVP shall not be present.
S-CSCF Name (See 7.4)	Server-Name	C	Name of the assigned S-CSCF. This AVP shall be present, if the requesting S-CSCF name is different from the previously assigned S-CSCF name stored in the HSS.

Wildcarded Public Identity (See 7.2b)	Wildcarded-Public-Identity	C	This AVP shall be present if: - the value of Server-Assignment-Type in the request was UNREGISTERED_USER and - the Wildcarded-Public-Identity AVP in the request was not present and - the Public Identity in the request fell within the range of a Wildcarded Public User Identity in the HSS whose state is registered. If this element is present, it shall be used by the S-CSCF to identify the identity affected by the request.

6.1.2.1 Detailed behaviour

On registering/deregistering a Public Identity the S-CSCF shall inform the HSS. The same procedure is used by the S-CSCF to get the user information which contains the user profile and the charging information. The relevant user profile downloaded is described in more detailed in sections 6.5.1 and 6.6.

The Public-Identity AVP and User-Data AVPs in this command pair shall contain only one type of identities i.e. either only Public User Identities, or only Public Service Identities. User initiated Rregistration/deregistration procedures (i.e. server-assignment-type is set to RE_REGISTRATION, USER_DEREGISTRATION, etc.) shall only be allowed for distinct Public User Identities.

The HSS holds information about the state of registration of all the identities related to an IMS Subscription. The S-CSCF uses this procedure to update such states. For Shared Public User Identities, the S-CSCF shall initiate this procedure towards the HSS for each Private User Identity undergoing a Registration or Deregistration related to the Shared Public User Identity. For implicitly registered identities, the rules defined in Section 6.5.1 shall apply.

When the request message was received because of a terminating session request, the HSS may prioritise the received request message according to priority level received within the Session-Priority AVP.

The HSS shall, in the following order (in case of an error in any of the steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.229 [5]):

1. Check that the Public Identity and Private Identity exist in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. The HSS may check whether the Private and Public Identities received in the request are associated in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

3. If more than one Public-Identity AVP is present and the Server-Assignment-Type is one of the values defined in Table 6.1.2.1 as applying for only one identity, then the Result Code shall be set to DIAMETER_AVP_OCCURS_TOO_MANY_TIMES and no user information shall be returned.

4. The HSS shall check the Public Identity type received in the request.

 - If the identity in the request is a distinct Public User Identity, continue in step 5, otherwise the HSS shall check the server-assignment-type:

 If it indicates REGISTRATION, RE_REGISTRATION, USER_DEREGISTRATION, USER_DEREGISTRATION_STORE_SERVER_NAME, AUTHENTICATION_FAILURE or AUTHENTICATION_TIMEOUT, Experimental-Result-Code shall be set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE.

 - If the identity in the request is a Public Service Identity, then check if the PSI Activation State for that identity is active. If not, then the response shall contain Experimental-Result-Code set to DIAMETER_ERROR_USER_UNKNOWN.

5. Check the Server Assignment Type value received in the request:

 - If it indicates REGISTRATION or RE_REGISTRATION, the HSS shall check whether the Public Identity is assigned for the S-CSCF requesting the data.

 If there is already an S-CSCF assigned to the user and the requesting S-CSCF is not the same as the previously assigned S-CSCF, and IMS restoration procedures are not supported or the S-CSCF reassignment pending flag is not set, the HSS shall include the name of the previously assigned S-CSCF in the response

message and the Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

If there is already an S-CSCF assigned to the user and the requesting S-CSCF is not the same as the previously assigned S-CSCF and IMS restoration procedures are supported, and the S-CSCF reassignment pending flag is set, the HSS shall overwrite the S-CSCF name and shall reset the S-CSCF reassignment pending flag.

If there is no S-CSCF assigned to the user or the the requesting S-CSCF is the same as the previously assigned S-CSCF stored in the HSS, the HSS shall download the relevant user information taking into consideration the value set in the User-Data-Already-Available AVP (see sub-clause 6.6). The Result-Code shall be set to DIAMETER_SUCCESS and the HSS shall set the registration state of the Public User Identity as registered (if not already registered).If the S-CSCF Restoration Information is included in the request and the HSS implements IMS Restoration procedures, and if it is RE_REGISTRATION, the HSS shall store this information. If the Public User Identity's authentication pending flag which is specific for the Private User Identity is set, the HSS shall clear it. If there are multiple Private User Identities, which belong to the served IMS subscription the Associated-Identities AVP should be added to the answer message and it shall contain all Private User Identities associated to the IMS subscription. If the loose-route mechanism is required for the registered Public User Identities, the Loose-Route-Indication AVP shall be added to the answer message. If there are multiple Private User Identities being registered with the Public Identity received in the request message, and the IMS Restoration Procedures are supported in the HSS, the Associated-Registered-Identities AVP shall be added to the answer message and it shall contain all Private User Identities being registered with the Public Identity.

If it is REGISTRATION and the HSS implements IMS Restoration procedures, if multiple registration indication is included in the request and the Public User Identity is stored as registered in the HSS, and there is restoration information related to the Private User Identity, the HSS shall not overwrite the stored S-CSCF Restoration Information, instead, it shall send the stored S-CSCF restoration information together with the user profile in the SAA. The Experimental-Result-Code shall be set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE. Otherwise, the HSS shall store the received S-CSCF restoration information. The Result-Code shall be set to DIAMETER_SUCCESS.

- If it indicates UNREGISTERED_USER, the HSS shall check whether the Public Identity is assigned for the S-CSCF requesting the data.

 If there is already an S-CSCF assigned to the user and the requesting S-CSCF is not the same as the previously assigned S-CSCF, and IMS restoration procedures are not supported or the S-CSCF reassignment pending flag is not set, the HSS shall include the name of the previously assigned S-CSCF in the response message and the Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

 If there is already an S-CSCF assigned to the user and the requesting S-CSCF is not the same as the previously assigned S-CSCF and IMS restoration procedures are supported, and the S-CSCF reassignment pending flag is set, the HSS shall overwrite the S-CSCF name and shall reset the S-CSCF reassignment pending flag.

 If there is no S-CSCF assigned to the user or the requesting S-CSCF is the same as the previously assigned S-CSCF stored in the HSS, the HSS shall store the S-CSCF name.

 If the registration state of the Public Identity is not registered, the HSS shall set the registration state of the Public Identity as unregistered, i.e. registered as a consequence of an originating or terminating request and download the relevant user information. The Result-Code shall be set to DIAMETER_SUCCESS. If there are multiple Private User Identities associated to the Public User Identity in the HSS, the HSS shall arbitrarily select one of the Private User Identities and put it into the response message.

 If the registration state of the Public Identity is registered and IMS restoration procedures are not supported, the HSS shall set the registration state of the Public identity as unregistered and download the relevant user information. The Result-Code shall be set to DIAMETER_SUCCESS. If there are multiple Private User Identities associated to the Public User Identity in the HSS, the HSS shall arbitrarily select one of the Private User Identities and put it into the response message.

 If the registration state of the Public Identity is registered and IMS restoration procedures are supported, the HSS shall include in the response all S-CSCF Restoration Information related with the Public User Identity. If there is S-CSCF Restoration Information associated with several Private User Identities, the HSS shall

include all the S-CSCF Restoration Information groups in the response. The Experimental-Result-Code shall be set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE.

If there are multiple Private User Identities, which belong to the served IMS subscription the Associated-Identities AVP should be added to the answer message and it shall contain all Private User Identities associated to the IMS subscription.

If the S-CSCF receives a wildcarded public identity from the I-CSCF, the S-CSCF shall use this wildcarded public identity to fetch the user profile (i.e. by sending a Cx-SAR including Wildcarded-Public-Identity AVP if the profile is not available) and registration information locally stored.

Ifthe S-CSCF does not receive a wildcarded public identity, the S-CSCF shall not perform wildcarded public identity matching and shall use the public identity received instead to fetch the user profile (i.e. by sending a Cx-SAR without including Wildcarded-Public-Identity AVP if the profile is not available) and registration information.

NOTE 1: There may be SIP requests in which the S-CSCF does not receive information of a wildcarded public identity, e.g. originating call from an AS on behalf of a user.

NOTE 2: Since a distinct public identity falling into the range of a wildcarded public identity can have a different service profile, the S-CSCF does not perform the wildcarded public identity matching against the public identity received to avoid using the wrong service profile.

If the Wildcarded-Public-Identity AVP is not received and if the Public Identity falls within the range of a wildcarded public identity whose registration state is registered, the HSS shall not overwrite the registration state. The Result-Code shall be set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE and the HSS shall include the Wildcarded-Public-Identity AVP in the response. Upon reception of this error, the S-CSCF should behave as if it has received a wildcarded public identity in the first place.

- If it indicates TIMEOUT_DEREGISTRATION, USER_DEREGISTRATION, DEREGISTRATION_TOO_MUCH_DATA or ADMINISTRATIVE_DEREGISTRATION, the HSS shall check the registration state for all the Public Identities in the request. If the request did not contain Public Identities the HSS shall check the registration state of the Public Identities associated with the Private Identity identified in the request. For each Public Identity;-

 - if the registration state of the Public User Identity is Registered, the HSS shall check if the Public User Identity is currently registered with one or more Private User Identities.

 - If the Public User Identity is currently registered with only one Private User Identity, the HSS shall set the registration state of the Public User Identity to Not Registered and clear the S-CSCF name and any S-CSCF Restoration Information associated with the Public User Identity.

 - If the Public User Identity is currently registered with more than one Private User Identity, the HSS shall keep the registration state of the Public User Identity as Registered and retain the S-CSCF name associated with the Public User Identity. The HSS shall remove any S-CSCF Restoration Information associated to the registration of this Public User Identity with this Private User Identity.

 - if the registration state of the Public Identity is Unregistered, the HSS shall set the registration state of the Public Identity to Not Registered and clear the S-CSCF name associated with the Public Identity.

 The Result-Code shall be set to DIAMETER_SUCCESS

- If it indicates TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME or USER_DEREGISTRATION_STORE_SERVER_NAME the HSS decides whether to keep the S-CSCF name associated to the Private User Identity stored or not for all the Public User Identities that the S-CSCF indicated in the request. If no Public User Identity is present in the request, the Private User Identity shall be present.

 - If the HSS decides to keep the S-CSCF name stored the HSS shall keep the S-CSCF name stored for all the Public User Identities associated to the Private User Identity. The Result-Code shall be set to DIAMETER_SUCCESS.

 The HSS shall check if each Public User Identity in the request is currently registered with one or more Private User Identities. If the request did not contain Public User Identities the HSS shall check if each

Public User Identity associated with the Private User Identity in the request is currently registered with one or more Private User Identities. For each Public User Identity;-

- If only one Private User Identity associated with the Public User Identity is currently registered with the Public User Identity, the HSS shall set the registration state of the Public User Identity to Unregistered and clear any S-CSCF Restoration Information associated with the Public User Identity

- If more than one Private User Identity that shares that Public User Identity is currently registered with the Public User Identity the HSS shall keep the registration state of the Public User Identity as Registered. The HSS shall remove any S-CSCF Restoration Information associated to the registration of this Public User Identity with the Private User Identity in the request.

- If the HSS decides not to keep the S-CSCF name the Experimental-Result-Code shall be set to DIAMETER_SUCCESS_SERVER_NAME_NOT_STORED.

 The HSS shall check if each Public User Identity in the request is currently registered with one or more Private User Identities. If the request did not contain Public User Identities the HSS shall check if each Public User Identity associated with the Private User Identity in the request is currently registered with one or more Private User Identities. For each Public User Identity;-

 - If only one Private User Identity associated with the Public User Identity is currently registered with the Public User Identity, the HSS shall set the registration state of the Public User Identity to Not Registered and clear the S-CSCF name associated with Public User Identity.

 - If more than one Private User Identity that shares that Public User Identity is currently registered with the Public User Identity the HSS shall keep the registration state of the Public User Identity as Registered.

- If it indicates NO_ASSIGNMENT, the HSS checks whether the Public Identity is assigned for the S-CSCF requesting the data. If the requesting S-CSCF is not the same as the assigned S-CSCF and the S-CSCF reassignment pending flag is not set, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY, otherwise the HSS shall download the relevant user information and the Result-Code shall be set to DIAMETER_SUCCESS. If relevant S-CSCF Restoration Information is stored in the HSS and IMS Restoration Procedures are supported, it shall be added to the answer message. If there is S-CSCF Restoration Information associated with several Private User Identities, the HSS shall include all the S-CSCF Restoration Information groups in the response. If there are multiple Private User Identities, which belong to the served IMS subscription the Associated-Identities AVP should be added to the answer message and it shall contain all Private User Identities associated to the IMS subscription.

NOTE 3: the check of the S-CSCF reassignment pending flag is needed since an S-CSCF supporting restoration procedures can receive a user initiated de-registration for a Public Identity for which it does not have any registration data (see 3GPP TS 23.380 [19]). In such case, the S-CSCF indicates NO_ASSIGNMENT in Server-Assignment-Type to retrieve any possible restoration information from the HSS.

- If it indicates AUTHENTICATION_FAILURE (e.g. there is a mismatch in IP-address secure binding information) or AUTHENTICATION_TIMEOUT (e.g. no response to Digest challenge), the HSS shall keep the registration state of the Public User Identity. The HSS shall check the registration state for the Public User Identity in the request and only if the registration state of the Public User Identity is Not Registered, the HSS shall clear the S-CSCF name associated with the Public User Identity.

 If the Public User Identity's authentication pending flag which is specific for the Private User Identity is set, the HSS shall clear it. The Result-Code shall be set to DIAMETER_SUCCESS.

If the HSS cannot fulfil the received request, e.g. due to database error, it shall set the Result-Code to DIAMETER_UNABLE_TO_COMPLY. The HSS shall not modify any registration state nor download any Public Identity information to the S-CSCF.

See chapter 8.1.2 and 8.1.3 for the description of the handling of the error situations: reception of an S-CSCF name different from the one stored in the HSS and reception of a Server-Assignment-Type value not compatible with the registration state of the Public Identity.

6.1.3 Network initiated de-registration by the HSS, administrative

In case of network initiated de-registration of by the HSS, the HSS change the state of the Public Identities to Not Registered and send a notification to the S-CSCF indicating the identities that shall be de-registered. The procedure is invoked by the HSS, corresponds to the functional level operation Cx-Deregister (see 3GPP TS 23.228 [1]).

This procedure is mapped to the commands Registration-Termination-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.1.3.1 and 6.1.3.2 describe the involved information elements.

Table 6.1.3.1: Network Initiated Deregistration by HSS request

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity / Public Service Identity (See 7.2 and 7.2a)	Public-Identity	C	It contains the list of Public Identities that are de-registered, in the form of SIP URL or TEL URL. Public-Identity AVP shall be present if the de-registration reason code is NEW_SERVER_ASSIGNED. It may be present with the other reason codes.
Private User Identity / Private Service Identity (See 7.3 and 7.3a)	User-Name	M	It contains the Private Identity in the form of a NAI. The HSS shall always send a Private Identity that is known to the S-CSCF based on an earlier SAR/SAA procedure.
Reason for de-registration (See 7.11)	Deregistration-Reason	M	The HSS shall send to the S-CSCF a reason for the de-registration. The de-registration reason is composed of two parts: one textual message (if available) that is intended to be forwarded to the user that is de-registered, and one reason code (see 3GPP TS 29.229 [5]) that determines the behaviour of the S-CSCF.
Routing Information (See 7.13)	Destination-Host	M	It contains the name of the S-CSCF which originated the last update of the name of the multimedia server stored in the HSS for a given IMS Subscription. The address of the S-CSCF is the same as the Origin-Host AVP in the message sent from the S-CSCF.
Associated Private Identities	Associated-Identities	O	This AVP contains Private Identities, which belong to the same IMS subscription as the Private Identity in the User-Name AVP and should be de-registered together with that one. If the IMS subscription contains only a single Private Identity, this AVP shall not be present.

Table 6.1.3.2: Network Initiated Deregistration by HSS response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / Experimental-Result	M	This information element indicates the result of de-registration. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
Associated Private Identities	Associated-Identities	C	This AVP shall be present if the S-CSCF de-registered more than one Private Identity with the request. It contains all Private Identities that have been deregistered together with the one in the User-Name AVP of the request.
Identities with Emergency Registration (See 7.25)	Identity-with-Emergency-Registration	C	This information element indicates a list of pairs of private and public user identities which have not been de-registered due to emergency registration. If IMS Restoration Procedures are supported, this information element also contains restoration information relevant to the emergency registrations.

6.1.3.1 Detailed behaviour

The HSS shall de-register the affected identities and invoke this procedure to inform the S-CSCF. The S-CSCF shall remove all the information stored in the S-CSCF for the affected identities.

The HSS may de-register:

- One Public Identity or a list of Public Identities. HSS may include all Public User Identities associated with the User-Name AVP to the request. This option is applicable with all reason codes.

- One or more Private Identities of the IMS Subscription with all associated Public Identities. No Public-Identity AVPs shall be present in this case. This option is applicable with reason codes PERMANENT_TERMINATION, SERVER_CHANGE, and REMOVE_S-CSCF.

- All Public Service Identities that match a Wildcarded Public Service Identity. In this case the HSS may send one of the Public Service Identities that was received in the Server Assignment Request for that Wildcarded Public Service Identity and the associated Private Service Identity.

- A Wildcarded Public User Identity. In this case the HSS shall send a distinct Public User Identity that belongs to the same implicit registration set as the Wildcarded Public User Identity and the associated Private User Identity.

The HSS shall send in the Deregistration-Reason AVP the reason for the de-registration, composed by a textual message (if available) aimed for the user and a reason code that determines the action the S-CSCF has to perform. The possible reason codes are:

- PERMANENT_TERMINATION: The HSS indicates to the S-CSCF that the S-CSCF will no longer be assigned to the Public Identity and associated implicitly registered Public Identities for the Private Indentity(ies) indicated in the request (e.g. due to an IMS subscription modification or a removal of IP-address secure binding information when GIBA is used).

 The HSS shall check the registration state of the Public Identities. If no Public Identities are involved, the HSS shall check the registration state of the Public Identities associated with the Private User Identity identified. For each Public Identity:

 - If the registration state of the Public Identity is Registered, the HSS shall check if the Public User Identity is currently registered with one or more Private User Identities.

 - If the Public User Identity is currently registered with only one Private User Identity, the HSS shall clear the S-CSCF name associated with the Public User Identity, and set the registration state of the Public User Identity to Not Registered (only if S-CSCF does not return Identities with Emergency Registrations in the response). The S-CSCF initiates the de-registration of the Public User Identity unless it is emergency registered.

 - If the Public User Identity is currently registered with more than one Private User Identity, the HSS shall keep the registration state of the Public User Identity as Registered and retain the S-CSCF name associated with the Public User Identity. The S-CSCF initiates the de-registration of the Public User Identity unless it is emergency registered.

 - If the registration state of the Public Identity is Unregistered, the HSS shall set the registration state of the Public Identity to Not Registered and clear the S-CSCF name associated with the Public Identity.

- NEW_SERVER_ASSIGNED: The HSS indicates to the S-CSCF that a new S-CSCF has been allocated to the IMS Subscription e.g. because the previous assigned S-CSCF was unavailable during a registration procedure. The S-CSCF shall remove all information for all of the Public Identities indicated in the request.

- SERVER_CHANGE: The HSS indicates to the S-CSCF that the de-registration is requested to force the selection of new S-CSCF to assign to the IMS Subscription (e.g. when the S-CSCF capabilities are changed in the HSS or when the S-CSCF indicates that it has not enough memory for the updated User Profile). The HSS shall set the registration state to "Not Registered" and clear the S-CSCF name for all of the Public Identities affected by the request. If the S-CSCF does not indicate in the response all the Private Identities that were in the request, the HSS shall repeat this request for each of the remaining Private Identities in the IMS Subscription that are known to the S-CSCF. The S-CSCF should start the network initiated de-registration towards the user, i.e. all registrations within the IMS Subscription are de-registered and the user is asked to re-register to all existing registrations.

- REMOVE_S-CSCF: The HSS indicates to the S-CSCF that the S-CSCF will no longer be assigned to an unregistered Public Identity(ies) (i.e registered as a consequence of an originating or terminating request or there is a S-CSCF keeping the user profile stored) for a given IMS Subscription. For each Public Identity contained within the request the HSS shall set the registration state of the Public Identity to Not Registered and clear the S-CSCF name associated with the Public Identity. The S-CSCF shall remove all information related to the Public User Identity contained within the request.

Public Identities which are emergency registered in the S-CSCF shall not be de-registered when a Cx-Deregistration request with a Deregistration-Reason of "PERMANENT_TERMINATION (0)" is received from the HSS. In this case

- if all to be de-registered identities are emergency registered, a result code of DIAMETER_UNABLE_TO_COMPLY and a list of Private / Public Identity pairs which are emergency registered shall be returned to the HSS

- if a proper subset of the to be de-registered entities are emergency registered, a result code of DIAMETER_LIMITED_SUCCESS and a list of Private Identity / Public Identity pairs which are emergency registered shall be returned to the HSS.

The HSS shall keep the registrations associated to the returned Private Identity / Public Identity pairs and shall not change their registration states. However, for cases of permanent subscription withdrawal the HSS is not expected to keep any data.

NOTE 1: If the Public Identity that is emergency registered has normal registration as well, then for the normal registration the S-CSCF will perform the detailed de-registration procedures towards the UE for each reason code as described in the 3GPP TS 24.229 [8].

NOTE 2: It is assumed that Public Identities which are implicitly registered along with an emergency registration are also emergency registered.

The detailed de-registration procedures performed by the S-CSCF for each reason code are described in the 3GPP TS 24.229 [8].

6.1.4 User location query

This procedure is used between the I-CSCF and the HSS to obtain the name of the S-CSCF assigned to a Public Identity, or the name of the AS hosting a PSI for direct routing. The procedure is invoked by the I-CSCF, is performed per Public Identity, and corresponds to the functional level operation Cx-Location-Query (see 3GPP TS 23.228 [1]).

This procedure is mapped to the commands Location Info Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.1.4.1 and 6.1.4.2 detail the involved information elements.

Table 6.1.4.1: User Location query

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity / Public Service Identity (See 7.2 and 7.2a)	Public-Identity	M	Public Identity
Routing information (See 7.13)	Destination-Host, Destination-Realm	C	If the I-CSCF knows HSS name Destination-Host AVP shall be present in the command. Otherwise, only Destination-Realm AVP shall be present and the command shall be routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the I-CSCF.
Originating Request (See 7.18)	Originating-Request	O	It indicates that the request is related to an originating SIP message.
Type of Authorization (See 7.14)	User-Authorization-Type	C	This information element shall be present and set to REGISTRATION_AND_CAPABILITIES by the I-CSCF if IMS Restoration Procedures are supported and the S-CSCF currently assigned to the Public User Identity in the HSS cannot be contacted.
Session Priority (See 7.24)	Session-Priority	O	This information element shall indicate the session's priority to the HSS. If it is not included, the request shall be treated as normal.

Table 6.1.4.2: User Location response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.
S-CSCF Name / AS name (See 7.4 and 7.4a)	Server-Name	C	Name of the assigned S-CSCF for basic IMS routing or the name of the AS for direct routing.
S-CSCF capabilities (See 7.5)	Server-Capabilities	O	It contains the information to help the I-CSCF in the selection of the S-CSCF.
Wildcarded Public Identity (See 7.2b)	Wildcarded-Public-Identity	O	If the requests refers to a Wildcarded PSI or Wildcarded Public User Identity (the Public Identity in the request matches a Wildcarded PSI or Wildcarded Public User Identity in the HSS), the HSS shall include the corresponding Wildcarded Public Identity in this information element. The matching of distinct Public Identies takes precedence over the matching of wildcarded public identities.

6.1.4.1 Detailed behaviour

The HSS may prioritise the received request message according to priority level received within the Session-Priority AVP.

The HSS shall, in the following order (if an error occurs in any of the steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.229 [5]):

1. Check that the Public Identity is known. If not the Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check the type of the Public Identity contained in the request:

 - If this is a Public User Identity, continue to step 2a.

- If this is a Public Service Identity:

 - Check if the PSI Activation State for that identity is active. If not, then the response shall contain Experimental-Result-Code set to DIAMETER_ERROR_USER_UNKNOWN.

 - Check if the name of the AS hosting the Public Service Identity is stored in the HSS and that the request does not contain the Originating-Request AVP. If this is the case the HSS shall return the AS name and the Result-Code AVP shall be set to DIAMETER_SUCCESS. Otherwise, continue to step 2a.

2a. Check if User-Authorization-Type was received in the request, and if the value is REGISTRATION_AND_CAPABILITIES:

- If it is, then the HSS shall return the Server-Capabilities AVP. If restoration procedures are supported, the HSS shall set the S-CSCF reassignment pending flag and allow overwriting of the S-CSCF name in the next SAR request, which enables the I-CSCF to select an S-CSCF. The returned capabilities must satisfy all the requirements of all the service profiles associated with the IMS Subscription. The Server-Capabilities AVP may be absent, to indicate to the I-CSCF that it can select any available S-CSCF. Result-Code shall be set to DIAMETER_SUCCESS. The HSS shall not return any S-CSCF name. Stop processing.

- Otherwise, continue to step 3.

3. Check the state of the Public Identity received in the request, and where necessary, check if the Public Identity has terminating services related to the unregistered state.

- If it is registered, the HSS shall return the stored S-CSCF name. The Server-Name AVP shall contain the SIP URI of the server. The Server-Capabilities AVP shall not be present. The Result-Code AVP shall be set to DIAMETER_SUCCESS.

- If it is unregistered (i.e. registered as a consequence of an originating or terminating request or there is a S-CSCF keeping the user profile stored) the HSS shall return the S-CSCF name assigned for that Public Identity. The Server-Name AVP shall contain the SIP URI of the server. The Server-Capabilities AVP shall not be present. The Result-Code shall be set to DIAMETER_SUCCESS.

- If it is not registered, but either it has terminating services related to unregistered state or the request contains the Originating-Request AVP, the HSS shall check if there is at least one Public Identity within the IMS Subscription with an S-CSCF name assigned:

 - If this is the case the HSS shall return the S-CSCF name assigned for that Public Identity. The Server-Name AVP shall contain the SIP URI of the server. The Server-Capabilities AVP shall not be present. The Result-Code shall be set to DIAMETER_SUCCESS.

 - If there is not any S-CSCF name assigned to a Public Identity within the IMS Subscription, the HSS may return information about the required S-CSCF capabilities, which enables the I-CSCF to select an S-CSCF. The Server-Capabilities AVP may be present. The HSS shall send the same server capability set that is sent in the user registration status response during the registration. If Server-Capabilities AVP is not present, the I-CSCF shall understand that any S-CSCF is suitable for the IMS Subscription. The Server-Name AVP shall not be present. The Experimental-Result-Code shall be set to DIAMETER_UNREGISTERED_SERVICE.

- If it is not registered or unregistered, and the Public Identity has no terminating services related to the unregistered state and the request does not contain the Originating-Request AVP, the response shall contain Experimental-Result-Code set to DIAMETER_ERROR_IDENTITY_NOT_REGISTERED.

If the HSS cannot fulfil the received request, e.g. due to database error, it shall set Result-Code to DIAMETER_UNABLE_TO_COMPLY. No S-CSCF name or S-CSCF capabilities shall be present in the response.

6.2 User data handling procedures

6.2.1 User Profile download

As part of the registration procedure (3GPP TS 23.228 [1]) S-CSCF obtains user data and service related information by means of the Cx-Put Resp operation (see 6.1.2).

6.2.2 HSS initiated update of User Profile

This procedure is initiated by the HSS to update user profile information and/or charging information and/or SIP Digest authentication information in the S-CSCF. This procedure corresponds to the functional level operation Cx-Update_Subscr_Data (see 3GPP TS 23.228 [1]).

This procedure is mapped to the commands Push-Profile-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.2.2.1 and 6.2.2.2 describe the involved information elements.

Table 6.2.2.1: User Profile Update request

Information element name	Mapping to Diameter AVP	Cat.	Description
Private User Identity / Private Service Identity (See 7.3 and 7.3a)	User-Name	M	Private Identity. The HSS shall always send a Private Identity that is known to the S-CSCF based on an earlier SAR/SAA procedure.
User profile (See 7.7)	User-Data	C	Updated user profile (see sections 6.5.2.1 and 6.6.1), with the format defined in chapter 7.7. It shall be present if the user profile is changed in the HSS. If the User-Data AVP is not present, the SIP-Auth-Data-Item or Charging-Information AVP shall be present.
Authentication Data (See 7.9)	SIP-Auth-Data-Item	C	SIP Digest authentication information. It shall be present if the used authentication scheme is SIP Digest and when password change has occurred in the HSS. If the SIP-Auth-Data-Item AVP is not present, the Charging-Information or User-Data AVP shall be present. See Table 6.3.6 for the contents of this information element.
Charging Information (See 7.12)	Charging-Information	C	Addresses of the charging functions. It shall be present if the charging addresses are changed in the HSS. If the Charging-Information AVP is not present, the SIP-Auth-Data-Item or User-Data AVP shall be present. When this parameter is included, either the Primary-Charging-Collection-Function-Name AVP or the Primary-Event-Charging-Function-Name AVP shall be included. All other charging information shall be included if it is available.
Routing Information (See 7.13)	Destination-Host	M	It contains the name of the S-CSCF which originated the last update of the name of the multimedia server stored in the HSS for a given IMS Subscription. The address of the S-CSCF is the same as the Origin-Host AVP in the message sent from the S-CSCF.

Table 6.2.2.2: User Profile Update response

Information element name	Mapping to Diameter AVP	Cat.	Description
Result (See 7.6)	Result-Code / Experimental-Result	M	This information element indicates the result of the update of User Profile in the S-CSCF. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

6.2.2.1 Detailed behaviour

The HSS shall make use of this procedure to update the relevant user information to the S-CSCF. The user information contains the user profile. See chapters 6.5.2.1 and 6.6.1 for the rules of user profile updating. If there are multiple registered Private User Identities associated to the Public User Identity in the HSS, the HSS shall send only single request and select arbitrarily one of the Private User Identities and put it into the request. For updates of the profile of a

Wildcarded Public Identity, the HSS shall send only one single request. That request shall contain the Wildcarded Public Identity (content within the Identity tag in the XML data shall be ignored by the S-CSCF).

The Charging-Information AVP and/or the User-Data AVP shall be present in the request. If the User-Data AVP is present in the request, the S-CSCF shall overwrite, for the Public Identities indicated in the User profile included in the request, current information with the information received from the HSS, except in the error situations detailed in table 6.2.2.1.1. If the Charging-Information AVP is present in the request, the S-CSCF shall replace the existing charging information with the information received from the HSS.

The SIP-Auth-Data-Item AVP shall be present if the command is sent in order to update SIP Digest authentication information due to a password change.

If the S-CSCF receives data that it can not recognise, unsupported user data in a part of the request where it may not be ignored or more data than it can accept, it shall return the corresponding error code to the HSS as indicated in table 6.2.2.1.1. The S-CSCF shall not overwrite the data that it already has to give service to the IMS Subscription. The HSS shall initiate a network-initiated de-registration procedure towards the S-CSCF with Deregistration-Reason set to SERVER_CHANGE, which will trigger the assignment of a new S-CSCF.

If the HSS receives DIAMETER_ERROR_USER_UNKNOWN from the S-CSCF in the Push-Profile-Answer, then the HSS shall re-send the request using another arbitrarily selected registered Private Identity (if any). If restoration procedures are not supported, the HSS shall set the unknown Private User Identity's registration status to "not registered"; this will allow the synchronization of the registration status in HSS and S-CSCF.

NOTE: If restoration procedures are supported, restoration procedures will ensure synchronization of the registration status in HSS and S-CSCF, i.e. the S-CSCF can either immediately retrieve the S-CSCF restoration information for the registered Public User Identity (sending SAR with Server Assignment Type set to NO_ASSIGNMENT), or wait for reception of a SIP request.

Table 6.2.2.1.1 details the valid result codes that the S-CSCF can return in the response.

Table 6.2.2.1.1: User profile response valid result codes

Result-Code AVP value	Condition
DIAMETER_SUCCESS	The request succeeded.
DIAMETER_ERROR_NOT_SUPPORTED_USER_DATA	The request failed. The S-CSCF informs the HSS that the received user information contained information, which was not recognised or supported by the S-CSCF due to unsupported S-CSCF capabilities.
DIAMETER_ERROR_USER_UNKNOWN	The request failed because the Private Identity is not found in S-CSCF.
DIAMETER_ERROR_TOO_MUCH_DATA	The request failed. The S-CSCF informs to the HSS that it tried to push too much data into the S-CSCF.
DIAMETER_UNABLE_TO_COMPLY	The request failed.

6.3 Authentication procedures

This procedure is used between the S-CSCF and the HSS to exchange information to support the authentication between the end user and the home IMS network. The procedure is invoked by the S-CSCF, corresponds to the combination of the operations Cx-AV-Req and Cx-AV-Req-Resp (see 3GPP TS 33.203 [3]) and is used:

- To retrieve authentication vectors from the HSS.
- To resolve synchronization failures between the sequence numbers in the UE and the HSS for authentication schemes that support this capability (e.g. IMS-AKA).
- To promote the result of the NASS-level authentication to the IMS level.
- To retrieve the IP-address secure binding information for GPRS-IMS-Bundled Authentication (GIBA) from the HSS.

This procedure is mapped to the commands Multimedia-Auth-Request/Answer in the Diameter application specified in 3GPP TS 29.229 [5]. Tables 6.3.1through 6.3.7 detail the involved information elements. Tables 6.3.1, 6.3.2 and 6.3.4 are common to all authentication schemes; Tables 6.3.3 and 6.3.5 are specific to IMS-AKA authentication; Tables 6.3.6 and 6.3.7 are specific to SIP Digest Authentication, when utilized. Table 6.3.8 is specific to NASS Bundled authentication, when utilized. Table 6.3.9 is specific to GPRS-IMS-Bundled Authentication (GIBA), when utilized.

Table 6.3.1: Authentication Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Public User Identity (See 7.2)	Public-Identity	M	This information element contains the Distinct Public User Identity of the user
Private User Identity (See 7.3)	User-Name	M	This information element contains the Private User Identity
Number Authentication Items (See 7.10)	SIP-Number-Auth-Items	M	This information element indicates the number of authentication vectors requested. Certain authentication schemes do not support more than one set of authentication vectors (e.g. SIP Digest, GIBA).
Authentication Data (See 7.9)	SIP-Auth-Data-Item	M	See Tables 6.3.2 and 6.3.3 for the contents of this information element. The content shown in table 6.3.2 shall be used for a normal authentication request; the content shown in table 6.3.3 shall only be used for an IMS-AKA authentication request after synchronization failure.
S-CSCF Name (See 7.4)	Server-Name	M	This information element contains the name (SIP URL) of the S-CSCF.
Routing Information (See 7.13)	Destination-Host	C	If the S-CSCF knows the HSS name this AVP shall be present. This information is available if the MAR belongs to an already existing registration, e.g. in case of the re-registration, where the HSS name is stored in the S-CSCF. The HSS name is obtained from the Origin-Host AVP, which is received from the HSS, e.g. included in the MAA command. This information may not be available if the command is sent in case of the initial registration. In this case the Destination-Host AVP is not present and the command is routed to the next Diameter node, e.g. SLF, based on the Diameter routing table in the client.

Table 6.3.2: Authentication Data content – Request

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	This information element indicates the authentication scheme. It shall contain: - "Digest-AKAv1-MD5" if the S-CSCF knows that IMS-AKA is to be used. - "SIP Digest" if the S-CSCF knows that SIP Digest is to be used. - "NASS-Bundled" if the S-CSCF knows that NASS Bundled authentication is to be used. - "Early-IMS-Security" if the S-CSCF knows that GPRS-IMS-Bundled Authentication is to be used. - "Unknown" if the S-CSCF can not know the authentication scheme at this point.
Authentication Context (See 7.9.7)	SIP-Authentication-Context	C	It shall contain authentication-related information relevant for performing the authentication. When Authentication Scheme contains "Digest-AKAv1-MD5", this AVP is not used and shall be missing.

Table 6.3.3: Authentication Data content – Request: Synchronization Failure for IMS-AKA

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. It shall contain "Digest-AKAv1-MD5".
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain the concatenation of RAND, as sent to the terminal, and AUTS, as received from the terminal. RAND and AUTS shall both be binary encoded. See 3GPP TS 33.203 [3] for further details about RAND and AUTS. The Authorization Information has a fixed length of 30 octets; the 16 most significant octets shall contain the RAND, the 14 least significant octets shall contain the AUTS.

Table 6.3.4: Authentication Request Response

Information element name	Mapping to Diameter AVP	Cat.	Description
User Identity **(See 7.2)**	**Public-Identity**	C	Public User Identity. It shall be present when the result is DIAMETER_SUCCESS.
Private User Identity **(See 7.3)**	**User-Name**	C	Private User Identity. It shall be present when the result is DIAMETER_SUCCESS.
Number Authentication Items (See 7.10)	**SIP-Number-Auth-Items**	C	This AVP indicates the number of authentication vectors delivered in the Authentication Data information element. It shall be present when the result is DIAMETER_SUCCESS. For SIP Digest, NASS Bundled authentication and GIBA this AVP shall be set to a value of 1.
Authentication Data (See 7.9)	SIP-Auth-Data-Item	C	If the SIP-Number-Auth-Items AVP is equal to zero or it is not present, then this AVP shall not be present. See Table 6.3.5 for the contents of this information element for IMS-AKA. See Table 6.3.6 for the contents of this information element for SIP Digest. See Table 6.3.8 for the contents of this information element for NASS Bundled authentication. See Table 6.3.9 for the contents of this information element for GIBA.
Result (See 7.6)	Result-Code / Experimental-Result	M	Result of the operation. Result-Code AVP shall be used for errors defined in the Diameter Base Protocol. Experimental-Result AVP shall be used for Cx/Dx errors. This is a grouped AVP which contains the 3GPP Vendor ID in the Vendor-Id AVP, and the error code in the Experimental-Result-Code AVP.

Table 6.3.5: Authentication Data content – Response for IMS-AKA

Information element name	Mapping to Diameter AVP	Cat.	Description
Item Number (See 7.9.1)	SIP-Item-Number	C	This information element shall be present in a SIP-Auth-Data-Item grouped AVP in circumstances where there are multiple occurrences of SIP-Auth-Data-Item AVPs, and the order in which they should be processed is significant. In this scenario, SIP-Auth-Data-Item AVPs with a low SIP-Item-Number value should be processed before SIP-Auth-Data-Items AVPs with a high SIP-Item-Number value.
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. It shall contain "Digest-AKAv1-MD5".
Authentication Information (See 7.9.3)	SIP-Authenticate	M	It shall contain, binary encoded, the concatenation of the authentication challenge RAND and the token AUTN. See 3GPP TS 33.203 [3] for further details about RAND and AUTN. The Authentication Information has a fixed length of 32 octets; the 16 most significant octets shall contain the RAND, the 16 least significant octets shall contain the AUTN.
Authorization Information (See 7.9.4)	SIP-Authorization	M	It shall contain, binary encoded, the expected response XRES. See 3GPP TS 33.203 [3] for further details about XRES.
Confidentiality Key (See 7.9.5)	Confidentiality-Key	O	This information element, if present, shall contain the confidentiality key. It shall be binary encoded.
Integrity Key (See 7.9.6)	Integrity-Key	M	This information element shall contain the integrity key. It shall be binary encoded.

Table 6.3.6: Authentication Data content – Response for SIP Digest

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	This information element indicates the authentication scheme. It shall contain "SIP Digest".
Digest Authenticate (See 7.9.8)	SIP-Digest-Authenticate	M	See Table 6.3.7 for contents of this information element.

Table 6.3.7: Digest Authenticate content – Response for SIP Digest

Information element name	Mapping to Diameter AVP	Cat.	Description
Digest Realm (See 7.9.8.1)	Digest-Realm	M	This information element corresponds to the realm parameter as defined in IETF RFC 2617 [16].
Digest Algorithm (See 7.9.8.3)	Digest-Algorithm	O	This information element contains the algorithm as defined in IETF RFC 2617 [16]. If this information element is not present, then "MD5" is assumed. If this information element is present it shall contain "MD5".
Digest QoP (See 7.9.8.4)	Digest-QoP	M	This information element contains the qop as defined in IETF RFC 2617 [16]. This information element shall be set to a value of "auth" by the HSS.
Digest HA1 (See 7.9.8.5)	Digest-HA1	M	This information element contains the H(A1) as defined in IETF RFC 2617 [16].

Table 6.3.8: Authentication Data content – Response for NASS-Bundled Authentication

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. It shall contain "NASS-Bundled".
Line Identifier (See 7.9.9)	Line-Identifier	M	This information element contains fixed broadband access line identifier associated to the user. This information element can be repeated.

Table 6.3.9: Authentication Data content – Response for GPRS-IMS-Bundled Authentication

Information element name	Mapping to Diameter AVP	Cat.	Description
Authentication Scheme (See 7.9.2)	SIP-Authentication-Scheme	M	Authentication scheme. For GPRS-IMS-Bundled Authentication it shall contain "Early-IMS-Security"
User IPv4 Address	Framed-IP-Address	C	If the IP Address of the User is an IPv4 address, this AVP shall be included. For a description of the AVP see IETF RFC 4005 [21].
User IPv6 Prefix	Framed-IPv6-Prefix	C	If the IP Address of the User is an IPv6 address, this AVP shall be included. For a description of the AVP see IETF RFC 4005 [21].
Framed Interface Id	Framed-Interface-Id	C	If and only if the IP Address of the User is an IPv6 address and the Framed-IPv6-Prefix AVP alone is not unique for the user this AVP shall be included. For a description of the AVP see IETF RFC 4005 [21].

6.3.1 Detailed behaviour

The HSS shall, in the following order (in case of an error in any of the steps the HSS shall stop processing and return the corresponding error code, see 3GPP TS 29.229 [5]):

1. Check that the Private User Identity and the Public User Identity exist in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

2. Check that the Public User Identity matches a distinct Public User Identity in the HSS. If it doesn't, the Experimental-Result-Code shall be set to DIAMETER_ERROR_USER_UNKNOWN.

3. Check whether the Private and Public User Identities in the request are associated in the HSS. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_IDENTITIES_DONT_MATCH.

4. Check the authentication scheme indicated in the request, and

 - if it is "Unknown", check the authentication scheme stored in HSS. If it is neither NASS-Bundled authentication nor SIP Digest authentication, Experimental-Result-Code shall be set to DIAMETER_ERROR_AUTH_SCHEME_UNSUPPORTED.

 - if not, check that the authentication scheme indicated in the request is supported. If not Experimental-Result-Code shall be set to DIAMETER_ERROR_AUTH_SCHEME_UNSUPPORTED.

This step is only applicable for IMS-AKA authentication. If the request indicates there is a synchronization failure, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

- If they are identical the HSS shall process AUTS as described in 3GPP TS 33.203 [3] and return the requested authentication information. The Result-Code shall be set to DIAMETER_SUCCESS.

5. Check the registration status of the Public User Identity received in the request:

 - If it is registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

 - If they are different, the HSS shall overwrite the S-CSCF name. If IMS restoration procedures are supported and the S-CSCF reassignment pending flag is set, the HSS shall reset the flag and keep the S-CSCF restoration information associated with the Public User Identity. The HSS shall download SIP-Auth-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. If authentication scheme is neither NASS-Bundled nor GIBA, the HSS shall set the Public User Identity's authentication pending flag which is specific to the Private User Identity received in the request. The Result-Code shall be set to DIAMETER_SUCCESS.

 - If they are identical, the HSS shall download SIP-Auth-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. The Result-Code shall be set to DIAMETER_SUCCESS.

 - If it is unregistered (i.e. registered as a consequence of an originating or terminating request or there is an S-CSCF keeping the user profile stored) or not registered, the HSS shall compare the S-CSCF name received in the request to the S-CSCF name stored in the HSS:

 - If they are different or if there is no S-CSCF name stored in the HSS for any Public User Identity of the IMS subscription, the HSS shall store the S-CSCF name. The HSS shall download SIP-Auth-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. If authentication scheme is neither NASS-Bundled nor GIBA, the HSS shall set the Public User Identity's authentication pending flag which is specific to the Private User Identity which was received in the request. The Result-Code shall be set to DIAMETER_SUCCESS.

 - If they are identical, the HSS shall download SIP-Auth-Data-Item stored up to a maximum specified in SIP-Number-Auth-Items received in the command Multimedia-Auth-Request. If authentication scheme is neither NASS-Bundled nor GIBA, the HSS shall set the Public User Identity's authentication pending flag which is specific to the Private User Identity that was received in the request. The Result-Code shall be set to DIAMETER_SUCCESS.

Exceptions to the cases specified here shall be treated by HSS as error situations, the Result-Code shall be set to DIAMETER_UNABLE_TO_COMPLY. No authentication information shall be returned.

6.4 User identity to HSS resolution

The User identity to HSS resolution mechanism enables the I-CSCF and the S-CSCF to find the identity of the HSS, that holds the subscriber data for a given Public Identity when multiple and separately addressable HSSs have been deployed by the network operator. The resolution mechanism is not required in networks that utilise a single HSS. An example for a single HSS solution is server farm architecture.

The resolution mechanism described in 3GPP TS 23.228 [1] shall use a Subscription Locator Function (SLF) or a Diameter Proxy Agent.

The I-CSCF and the S-CSCF accesses the SLF via the Dx interface. The Dx interface shall always be used in conjunction with the Cx interface. The Dx interface shall be based on Diameter. The SLF functionality shall use the routing mechanism provided by an enhanced Diameter redirect agent.

The SLF or the Diameter Proxy Agent shall be able to determine the HSS identity.

To get the HSS identity the I-CSCF and the S-CSCF shall send the Cx request normally destined to the HSS to a pre-configured Diameter address/name.

- If this Cx Request is received by an SLF (acting as a Diameter redirect agent), the SLF shall determine the HSS identity and sends to the I-CSCF or S-CSCF a notification of redirection towards the HSS identity, in response to

the Cx request. Multiple HSS identities may be included in the response, as specified in IETF RFC 3588 [9]. In such a case, the I-CSCF or the S-CSCF shall send the Cx Request to the first HSS identity in the ordered list received in the Cx Response from the SLF. If the I-CSCF or S-CSCF does not receive a successful response to the Cx Request, the I-CSCF or S-CSCF shall send a Cx Request to the next HSS identity in the ordered list. This procedure shall be repeated until a successful response from an HSS is received.

- If this Cx Request is received by the Diameter Proxy Agent, the Diameter Proxy Agent shall determine the HSS identity and shall forward the Cx request directly to the HSS. The I-CSCF and S-CSCF shall determine the HSS identity from the response to the Cx request received from the HSS.

While the I-CSCF is stateless, the S-CSCF shall store the HSS identity/name/Realm, as specified in 3GPP TS 23.228 [1] and shall use it in further Cx requests associated to the same IMS Public Identity.

In networks where the use of the user identity to HSS resolution mechanism is required, each I-CSCF and S-CSCF shall be configured with the address/name of the SLF or the Diameter Proxy Agent to enable use of these resolution mechanisms.

6.5 Implicit registration

Implicit registration is the mechanism by which a user is allowed to register simultaneously more than one of his/her Public User Identities. The HSS knows the identities that are to be implicitly registered when it receives the indication of the registration of an individual identity.

What follows is an extension of the affected basic procedures.

6.5.1 S-CSCF initiated procedures

The result of the S-CSCF initiated procedures affects all the Public User Identities that are configured in the HSS to be in the same implicitly registered Public User Identity set with the targeted individual Public User Identity. Where the S-CSCF initiated procedure affects the Registration state of the targeted Public User Identity, the Registration states of the Public User Identities in the associated implicitly registered Public User Identity set are affected in the same way.

6.5.1.1 Registration

The notification of a registration of a Public User Identity implies the registration of the corresponding implicitly registered Public User Identity set. The user information downloaded in the response contains the Public User Identities of the implicitly registered Public User Identity set with the associated service profiles. This allows the S-CSCF to know which Public User Identities belong to the implicitly registered Public User Identity set. The S-CSCF shall take from the set of implicitly registered Public User Identities the first identity which is not barred, and use this as the default Public User Identity. The default Public User Identity shall be a distinct Public User Identity.

6.5.1.2 De-registration

The de-registration of a Public User Identity implies the de-registration of the corresponding implicitly registered Public User Identity set, both in the HSS and in the S-CSCF. The S-CSCF shall include in the request a single Public User Identity to deregister all the Public User Identities that belong to the corresponding implicitly registered Public User Identity set.

The de-registration of a Private User Identity implies the de-registration of all the corresponding Public User Identities, both in the HSS and in the S-CSCF.

6.5.1.3 Authentication

Setting the authentication pending flag for a Public User Identity implies setting the authentication pending flag for each corresponding implicitly registered Public User Identity in the HSS.

6.5.1.4 Downloading the user profile

If the S-CSCF requests to download a user profile from HSS, the user profile in the response shall contain the Public User Identities of the corresponding implicitly registered Public User Identity set with the associated service profiles.

6.5.1.5 Initiation of a session to a non-registered user

The change of a Public User Identity to the Unregistered state due to the initiation of a session from/to a Public Identity that was in Not Registered state and the opposite change from Unregistered state to Not Registered state implies the same change for all the Public User Identities in the same Implicit Registration Set.

6.5.2 HSS initiated procedures

6.5.2.1 Update of User Profile

A request sent by the HSS to update the user profile shall include only the Public User Identities of the implicitly registered Public User Identity set, with the associated service profiles (even if not updated). If other Public User Identities not associated with the implicitly registered Public User Identity set are affected, they shall be downloaded in separate commands.

This procedure shall be used by the HSS to add a newly provisioned or Not Registered Public User Identity or Identities to an existing implicitly registered Public User Identity set that is in the state Registered or Unregistered. The added Public User Identity gets the registration state of the set it is added to.

The HSS shall use this procedure if a Public User Identity or Identities are removed from the implicitly registered Public User Identity set that is in a state Registered or Unregistered. In practise, this is done by sending a PPR for the set without the removed identities. The S-CSCF shall remove all information stored in the S-CSCF for the removed identities.

The HSS shall not use this procedure if there is no Public User Identities left in the implicitly registered Public User Identity set after the removal. In that case HSS shall use the RTR command instead.

The HSS shall not use this procedure to change the default Public User Identity of the implicitly registered Public User Identity set that is in a state Registered. In that case the HSS shall use the RTR command to de-register the Public User Identity set.

Moving of a Public User Identity or Identities from one implicitly registered Public User Identity set to another set shall be done in two steps: First the identity or identities are removed from the "old" set as described above, then the identity or identities are added to the "new" set as described above.

6.5.2.2 De-registration

A request sent by the HSS to de-register any of the identities included in an implicitly registered Public User Identity set shall affect all the Public User Identities of the deregistered set.

The de-registration of a Private User Identity implies the de-registration of all the corresponding Public User Identities, both in the HSS and in the S-CSCF.

6.5.2.3 Update of the Charging information

A request sent by the HSS to update the charging information shall include the Private User Identity for whom the charging information changed.

6.6 Download of the Relevant User Profile

The download of the relevant user profile from the HSS to the S-CSCF depends on whether the user profile is already stored in the S-CSCF. If the SiFC feature is supported by the HSS and S-CSCF, the HSS shall download the identifiers of the shared iFC sets. If either the HSS or the S-CSCF does not support the SiFC feature, the HSS shall download the complete iFCs, and SiFC identifiers shall not be downloaded by the HSS. The SiFC feature is defined in 3GPP TS 29.229 [5].

If User-Data-Already-Available is set to USER_DATA_NOT_AVAILABLE the HSS shall download the requested user profile. If the Public User Identity in the request is included in an implicitly registered Public User Identity set, the HSS shall include in the response the service profiles associated with all Public User Identities within the implicitly registered Public User Identity set to which the received Public User Identity belongs.

If User-Data-Already-Available is set to USER_DATA_ALREADY_AVAILABLE, the HSS should not return any user profile data. The HSS may override User-Data-Already-Available set to USER_DATA_ALREADY_AVAILABLE and download the user profile.

6.6.1 HSS initiated update of User Profile

The request to update the user profile in the S-CSCF includes only the Public User Identities of the implicitly registered Public User Identity set with the associated service profiles. See 6.5.2.1.

If the Public Identity is registered or unregistered (i.e. registered as a consequence of an originating or terminating request or there is a S-CSCF keeping the user profile stored) and there are changes in the user profile, the HSS should immediately push the complete user profile to the S-CSCF.

6.6.2 S-CSCF operation

At deregistration of a Public User Identity, the S-CSCF shall store the user information if it sends Server-Assignment-Request command including Server-Assignment-Type AVP set to value USER_DEREGISTRATION_STORE_SERVER_NAME or TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME and the HSS responds with DIAMETER_SUCCESS. Otherwise the S-CSCF shall not keep user information.

6.7 S-CSCF Assignment

The list of mandatory and optional capabilities received by an I-CSCF from the HSS allows operators to distribute users between S-CSCFs, depending on the different capabilities (e.g. features, role, geographical location) that each S-CSCF may have. Alternatively, an operator has the possibility to steer users to certain S-CSCFs.

The operator shall define (possibly based on the functionality offered by each S-CSCF installed in the network) the exact meaning of the S-CSCF mandatory and optional capabilities available in his network. It is an operator task to allocate a unique value to represent a single capability (e.g. support of "wildcarded PSI") or a set of capabilities (e.g. support of "alias" and "Shared IFC sets" and "wildcarded PSI") and to use these values to identify capabilities that are mandatory and/or optional to support for a given subscription. It is a configuration task for the operator to ensure that the I-CSCF has a correct record of the capabily values received from the HSS for each S-CSCF available in his network. The I-CSCF and the HSS do not need to know the semantic of these values. This semantic is exclusively an operator issue.

As a first choice, the I-CSCF shall select an S-CSCF that has all the mandatory and optional capabilities for the user. Only if that is not possible shall the I-CSCF apply a ‘best-fit’ algorithm. If more than one S-CSCF is identified that supports all mandatory capabilities the I-CSCF may then consider optional capabilities in selecting a specific S-CSCF. The ‘best-fit’ algorithm is implementation dependent and out of the scope of this specification.

It is the responsibility of the operator to ensure that there are S-CSCFs which have mandatory capabilities indicated by the HSS for any given user. However, configuration errors may occur. If such errors occur and they prevent the I-CSCF from selecting an S-CSCF which meets the mandatory capabilities indicated by the HSS, the I-CSCF shall inform the operator via the O&M subsystem.

As an alternative to selecting an S-CSCF based on the list of capabilities received from the HSS, it is possible to steer users to certain S-CSCFs. To do this, the operator may include one or more S-CSCF names as part of the capabilities of the user profile. The reason for the selection (e.g. all the users belonging to the same company/group could be in the same S-CSCF to implement a VPN service) and the method of selection are operator issues and out of the scope of this specification. If this alternative is chosen, the HSS shall include Server-Name AVPs in the Server-Capabilities AVP and should not include Mandatory-Capability AVPs or Optional-Capability AVPs in the Server-Capabilities AVP, and the I-CSCF when receiving Server-Name AVPs within the Server-Capabilities AVP shall discard any Mandatory-Capability AVP and any Optional-Capability AVP received within the Server-Capabilities AVP.

The following table is a guideline for operators that records S-CSCF capabilities that need to be supported by an S-CSCF in order to serve a user or a service (identified by a Public User Identity or Public Service Identity), that cannot be served by an S-CSCF which is only compliant to a previous 3GPP release.

Table 6.7: Guidelines for S-CSCF Capabilities

Capability	Mandatory or Optional (note)	Description
Support of "Wildcarded PSI"	M	This capability indicates that the assigned S-CSCF shall support the handling of Wildcarded PSIs.
Support of "OrigUnreg SPT"	M	This capability indicates that the assigned S-CSCF shall be able to process iFCs with a Session Case "Originating_Unregistered" received from the HSS in the user profile.
Support of "OrigCDIV SPT"	M	This capability indicates that the assigned S-CSCF shall be able to process iFCs with a Session Case "Originating_CDIV" received from the HSS in the user profile.
Support of "Shared iFC sets"	O	This capability indicates that the assigned S-CSCF may support the "SiFC" feature defined in the 3GPP TS 29.229 [5].
Support of "Display Name"	O	This capability indicates that the assigned S-CSCF may support the handling of "Display Name". The behaviour of the S-CSCF related to this missing data is the same as if the HSS did not send the Display Name.
Support of "Alias"	O	This capability indicates that the assigned S-CSCF may support the "AliasInd" feature defined in 3GPP TS 29.229 [5].
Support of "SIP Digest Authentication"	M	This capability indicates that the assigned S-CSCF shall support the handling of SIP Digest Authentication.
Support of "NASS Bundled Authentication"	M	This capability indicates that the assigned S-CSCF shall support the handling of NASS Bundled Authentication.
Support of "Wildcarded IMPUs"	M	This capability indicates that the assigned S-CSCF shall support the handling of Wildcarded Public User Identities.
Support of "Loose-Route "	M	This capability indicates that the assigned S-CSCF shall support the loose-route mechanism.
Support of "Service Level Trace"	M	This capability indicates that the assigned S-CSCF shall support the Service Level Trace mechanism.
Support of "Priority Service"	M	This capability indicates that the S-CSCF shall support the Service Priority Level indication. See IETF RFC 4412 [22] and 3GPP TS 24.229 [8].
Support of "Early IMS Security"	M	This capability indicates that the assigned S-CSCF shall support GIBA.

Note: Mandatory (M) corresponds to a Mandatory Capability that shall be supported by the assigned S-CSCF for a given user. The I-CSCF shall not select an S-CSCF that does not meet a mandatory capability. The selection of a S-CSCF not supporting this capability would lead to an unspecified network behaviour.

Optional (O) corresponds to an Optional Capability that may be supported by the assigned S-CSCF for a given user. The selection of a S-CSCF that would not support this capability will not significantly affect the network behaviour.

7 Information element contents

7.1 Visited Network Identifier

This information element contains the domain name of the visited network.

7.2 Public User Identity

This information element contains the Public User Identity. For definition of a Public User Identity, see 3GPP TS 23.003 [17].

When GPRS-IMS-Bundled Authentication (GIBA) is used, a Temporary Public User Identity is derived from the IMSI used for bearer network access according to the rules in 3GPP TS 23.003 [17].

7.2a Public Service Identity

This information element contains a Public Service Identity (PSI) that is hosted by an application server. For definition of a PSI, see 3GPP TS 23.003 [17].

7.2b Wildcarded Public Identity

This information element contains a Wildcarded PSI that is hosted by an application server or a Wildcarded Public User Identity. For definition of a Wildcarded PSI and a Wildcarded Public User Identity, see 3GPP TS 23.003 [17].

7.2c Void

7.3 Private User Identity

This information element contains the Private User Identity. For definition of a Private User Identity, see 3GPP TS 23.003 [17].

When GPRS-IMS-Bundled Authentication (GIBA) is used, the Private User Identity is derived from the IMSI as specified in 3GPP TS 33.203 [3].

7.3a Private Service Identity

This information element contains the Private Service Identity. For definition of a Private Service Identity, see 3GPP TS 23.003 [17].

7.4 S-CSCF Name

This information element contains the S-CSCF Name of the S-CSCF assigned to an IMS Subscription. For definition of a S-CSCF Name, see 3GPP TS 23.008 [18].

7.4a AS Name

This information element contains the AS Name of the AS hosting a Public Service Identity. For definition of AS Name, see 3GPP TS 23.008 [18].

7.5 S-CSCF Capabilities

This information element carries information to assist the I-CSCF during the process of selecting an S-CSCF for a certain IMS Subscription.

7.6 Result

This information element contains result of an operation. See 3GPP TS 29.229 [5] for the possible values.

7.7 User Profile

This information element contains the user profile in XML format. The user profile XML shall be valid against the user profile XML schema defined in Annex E.

Annex B specifies the UML logical model of the user profile downloaded via the Cx interface.

Annex D contains and informative, high level representation, of the wire representation of user profile data.

7.8 Server Assignment Type

Indicates the type of server assignment. See 3GPP TS 29.229 [5] for the list of existing values.

7.9 Authentication Data

This information element is composed of the following sub-elements.

7.9.1 Item Number

This information element indicates the order in which the authentication vectors are to be consumed.

7.9.2 Authentication Scheme

This information element contains the authentication scheme, which is used to encode the authentication parameters.

7.9.3 Authentication Information

This information element is used to convey the challenge and authentication token user during the authentication procedure. See 3GPP TS 33.203 [3] for details.

7.9.4 Authorization Information

This information element is used, in an authentication request, to indicate a failure of synchronization. In a response, it is used to convey the expected response to the challenge used to authenticate the user. See 3GPP TS 33.203 [3].

7.9.5 Confidentiality Key

This information element contains the confidentiality key. See 3GPP TS 33.203 [3].

7.9.6 Integrity Key

This information element contains the integrity key. See 3GPP TS 33.203 [3].

7.9.7 Authentication Context

This information element contains authentication-related information relevant for performing the authentication but that is not part of the SIP authentication headers. Some mechanisms (e.g. PGP, digest with quality of protection set to authint defined in IETF RFC 2617 [16], digest with predictive nonces or sip access digest) request that part or the whole SIP request (e.g. the SIP method) is passed to the entity performing the authentication. In such cases the SIPAuthentication-Context AVP shall be carrying such information.

7.9.8 Digest Authenticate

This information element is composed of the following sub-elements.

7.9.8.1 Digest Realm

This information element is part of the Digest authentication challenge, and corresponds to the realm parameter as defined in IETF RFC 3261 [11]. This information element is used to convey the realm to the S-CSCF during the SIP Digest authentication procedure.

7.9.8.2 Void

7.9.8.3 Digest Algorithm

This information element is part of the Digest authentication challenge, defined in IETF RFC 2617 [16].

7.9.8.4 Digest QoP

This information element is part of the Digest authentication challenge, defined in IETF RFC 2617 [16]. It provides the Quality of Protection indication and has an effect on the digest computation.

7.9.8.5 Digest HA1

This information element is part of the Digest authentication challenge, defined in IETF RFC 2617 [16].

7.9.9 Line Identifier

This information element contains the line identifier of the user's network termination.

7.10 Number Authentication Items

This information element contains the number of authentication vectors requested or delivered.

7.11 Reason for de-registration

This information element contains the reason for a de-registration procedure.

7.12 Charging information

Addresses of the charging functions. See 3GPP TS 29.229 [5].

7.13 Routing information

Information to route requests.

7.14 Type of authorization

Type of authorization requested by the I-CSCF. See 3GPP TS 29.229 [5] for a list of values.

7.15 Void

Void

7.16 User Data Already Available

This information element indicates to the HSS if the user profile is already available in the S-CSCF. See 3GPP TS 29.229 [5] for a list of values.

7.17 Associated Private Identities

This information element indicates to the S-CSCF the Private Identities, which belong to the same IMS Subscription as the Private Identity received in the request command. See 3GPP TS 29.229 [5].

7.18 Originating-Request

This information element indicates to the HSS that the request is related to an originating SIP message. See 3GPP 29.229 [5].

7.19 User Authorization Request Flags

This information element carries the following indication (see 3GPP 29.229 [5] for coding details):

- IMS Emergency Registration.

7.20 Loose-Route Indication

This information element indicates to the S-CSCF that the loose-route mechanism shall be applied to the public identities contained in the user profile received from the HSS. See 3GPP TS 29.229 [5]. This information is static data for the duration of the subscription or the validity of the IMS identity. Modification of this data result in Network Initiated Deregistration (SERVER_CHANGE); see section 6.1.3.1.

7.21 S-CSCF Restoration Information

This information element contains information for the S-CSCF to handle traffic for a registered user. It is associated with the Private User Identity and the Implicit Registration Set that is affected by the SAR request. See 3GPP TS 29.229 [5] for the contents of this information element.

7.22 Associated Registered Private Identities

This information element indicates to the S-CSCF the Registered Private Identities, which were registered with the Public Identity received in the request command. See 3GPP TS 29.229 [5].

7.23 Multiple Registration Indication

This information element indicates to the HSS that this is related to a multiple registration or to an emergency registration. See 3GPP TS 29.229 [5].

7.24 Session-Priority

This information element indicates the session's priority level to the HSS. See 3GPP TS 29.229 [5].

7.25 Identities with Emergency Registration

This information element indicates to the HSS a list of pairs of Private / Public Identities that are emergency registered. See 3GPP TS 29.229 [5].

8 Error handling procedures

8.1 Registration error cases

This section describes the handling of error cases, which can occur during the registration process. If the new and previously assigned S-CSCF names sent in the Multimedia-Auth-Request command are different and the Multimedia-Auth-Request is not indicating synchronisation failure (i.e. the request does not contain auts parameter), then the HSS shall overwrite the S-CSCF name.

If the new and previously assigned S-CSCF names sent in a command other than the Multimedia-Auth-Request command are different and the S-CSCF reassignment pending flag is not set, then the HSS shall not overwrite the S-CSCF name; instead it shall send a response to the S-CSCF indicating an error.

8.1.1 Cancellation of the old S-CSCF

It is possible that in certain situations the HSS receives a Multimedia-Auth-Request (MAR) command including a S-CSCF name, which is not the same as the previously assigned S-CSCF for the user. This can happen e.g. in case the new S-CSCF is selected due to a failure in the re-registration if the previously assigned S-CSCF does not respond to REGISTER message sent from the I-CSCF after a timeout.

In this case, the new S-CSCF is assigned for the user and if registrations in the previously assigned S-CSCF exist for the user, these registrations in the old S-CSCF are handled locally in the old S-CSCF, e.g. re-registration timers in the old S-CSCF shall cancel the registrations. Additionally, the HSS should de-register the registrations in the old S-CSCF by using the Registration-Termination-Request command. In this case, the HSS shall first check whether the deregistration is really required by comparing the Diameter client address of the newly assigned S-CSCF received in the MAR command to the Diameter client address stored in the HSS. If the Diameter client addresses match, the deregistration shall not be initiated. Otherwise the deregistration should be initiated for all the Public User Identities associated to the same Private User Identity, and if there is a Public User Identity shared by multiple Private User Identities, then the Registration-Termination-Request shall also be sent for all those Private User Identities. It shall be done in the following order:

1. Deregistration-Reason AVP value set to NEW_SERVER_ASSIGNED, for the Public User Identity, which is registered in the new S-CSCF.

2. Deregistration-Reason AVP value set to SERVER_CHANGE, for the user Public User Identities, which are not registered in the new S-CSCF.

8.1.2 Error in S-CSCF name

If the S-CSCF name sent in the Server-Assignment-Request command and the previously assigned S-CSCF name stored in the HSS are different and the S-CSCF reassignment pending flag is not set, then the HSS shall not overwrite the S-CSCF name. If the Server Assignment Type indicates NO_ASSIGNMENT, the HSS shall send a response to the S-CSCF with Result-Code value set to DIAMETER_UNABLE_TO_COMPLY. For all other Server Assignment Types, the HSS shall send a response to the S-CSCF with Experimental-Result-Code value set to DIAMETER_ERROR_IDENTITY_ALREADY_REGISTERED.

If the S-CSCF name sent in the Server-Assignment-Request command and the previously assigned S-CSCF name stored in the HSS are different and IMS Restoration Procedures are supported and the S-CSCF reassignment pending

flag is set, then the HSS shall allow overwriting of the S-CSCF name and proceed with the processing of the SAR command as defined in section 6.1.2.

8.1.3 Error in S-CSCF assignment type

If the Server-Assignment-Type in the Server-Assignment-Request command sent by the S-CSCF to the HSS is not allowed (i.e if the Server-Assignment-Type is not applicable based on the user state or it is not applicable based on the user identity type), the HSS shall send a response to the S-CSCF with the Experimental-Result-Code value set to DIAMETER_ERROR_IN_ASSIGNMENT_TYPE.

9 Protocol version identification

See 3GPP TS 29.229 [5].

10 Operational Aspects

See 3GPP TS 29.229 [5].

Annex A (normative): Mapping of Cx operations and terminology to Diameter

A.1 Introduction

This appendix gives mappings from Cx to Diameter protocol elements. Diameter protocol elements are defined in 3GPP TS 29.229 [5].

A.2 Cx message to Diameter command mapping

The following table defines the mapping between stage 2 operations and Diameter commands:

Table A.2.1: Cx message to Diameter command mapping

Cx message	Source	Destination	Command-Name	Abbreviation
Cx-Query + Cx-Select-Pull	I-CSCF	HSS	User-Authorization-Request	UAR
Cx-Query Resp + Cx-Select-Pull Resp	HSS	I-CSCF	User-Authorization-Answer	UAA
Cx-Put + Cx-Pull	S-CSCF	HSS	Server-Assignment-Request	SAR
Cx-Put Resp + Cx-Pull Resp	HSS	S-CSCF	Server-Assignment-Answer	SAA
Cx-Location-Query	I-CSCF	HSS	Location-Info-Request	LIR
Cx-Location-Query Resp	HSS	I-CSCF	Location-Info-Answer	LIA
Cx-AuthDataReq	S-CSCF	HSS	Multimedia-Authentication-Request	MAR
Cx-AuthDataResp	HSS	S-CSCF	Multimedia-Authentication-Answer	MAA
Cx-Deregister	HSS	S-CSCF	Registration-Termination-Request	RTR
Cx-Deregister Resp	S-CSCF	HSS	Registration-Termination-Answer	RTA
Cx-Update_Subscr_Data	HSS	S-CSCF	Push-Profile-Request	PPR
Cx-Update_Subscr_Data Resp	S-CSCF	HSS	Push-Profile-Answer	PPA

A.3 Cx message parameters to Diameter AVP mapping

The following table gives an overview about the mapping:

Table A.3.1: Cx message parameters to Diameter AVP mapping

Cx parameter	AVP Name
Visited Network Identifier	Visited-Network-Identifier
Public Identity	Public-Identity
Private Identity	User-Name
S-CSCF Name	Server-Name
AS Name	
S-CSCF capabilities	Server-Capabilities
Result	Result-Code
	Experimental-Result-Code
User profile	User-Data
Server Assignment Type	Server-Assignment-Type
Authentication data	SIP-Auth-Data-Item
Item Number	SIP-Item-Number
Authentication Scheme	SIP-Authentication-Scheme
Authentication Information	SIP-Authenticate
Authorization Information	SIP-Authorization
Confidentiality Key	Confidentiality-Key
Integrity Key	Integrity-Key
Number Authentication Items	SIP-Number-Auth-Items
Reason for de-registration	Deregistration-Reason
Charging Information	Charging-Information
Routing Information	Destination-Host
Type of Authorization	Authorization-Type
Associated Private Identities	Associated-Identities
Digest Authenticate	SIP-Digest-Authenticate
Digest Realm	Digest-Realm
Digest Algorithm	Digest-Algorithm
Digest QoP	Digest-QoP
Digest HA1	Digest-HA1
Line Identifier	Line-Identifier
Wildcarded Public Identity	Wildcarded-Public Identity
Loose-Route Indication	Loose-Route-Indication
S-CSCF Restoration Information	SCSCF-Restoration-Info
Multiple Registration Indication	Multiple-Registration-Indication

A.4 Message flows

The following message flows give examples regarding which Diameter messages shall be sent in scenarios described in 3GPP TS 23.228 [1].

A.4.1 Registration– user not registered

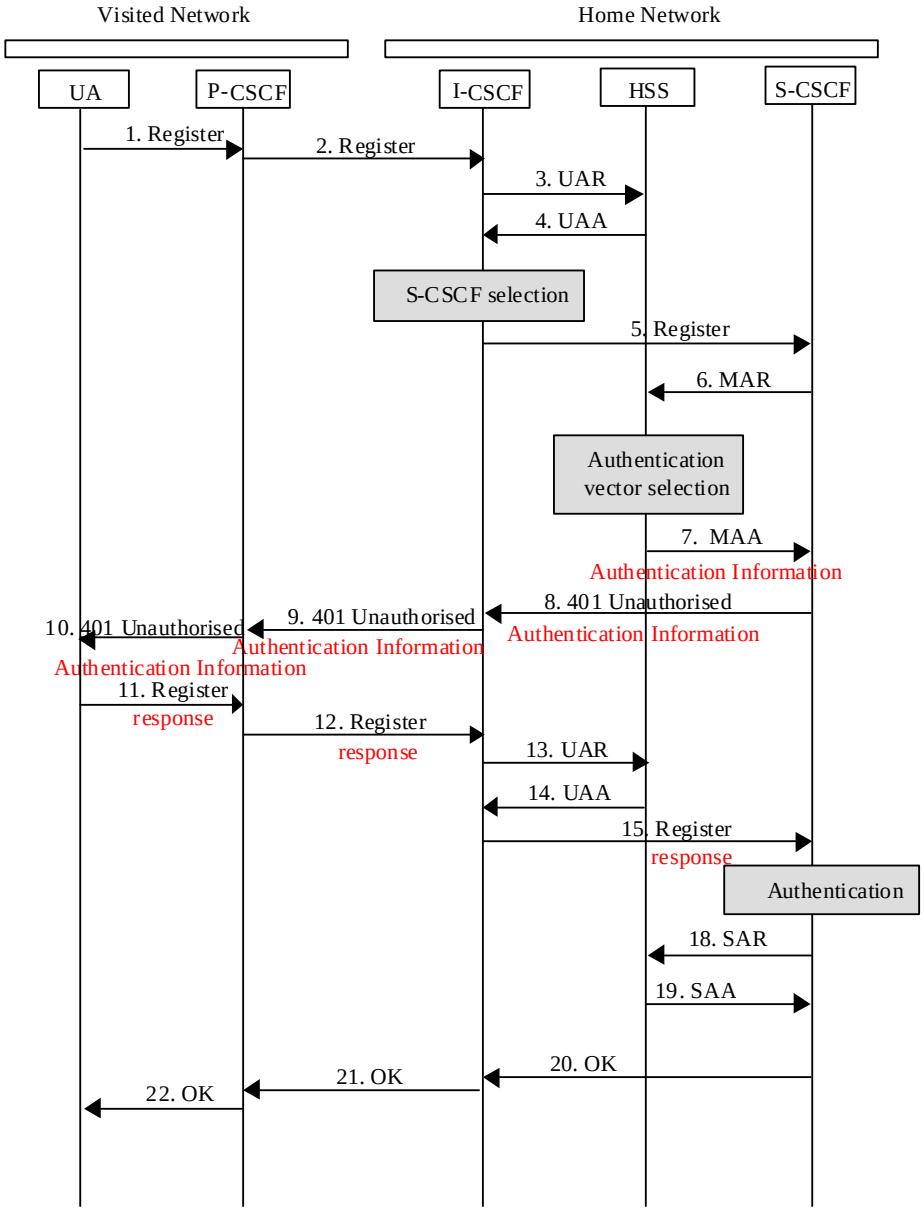


Figure A.4.1.1: Registration – user not registered

A.4.2 Registration – user currently registered

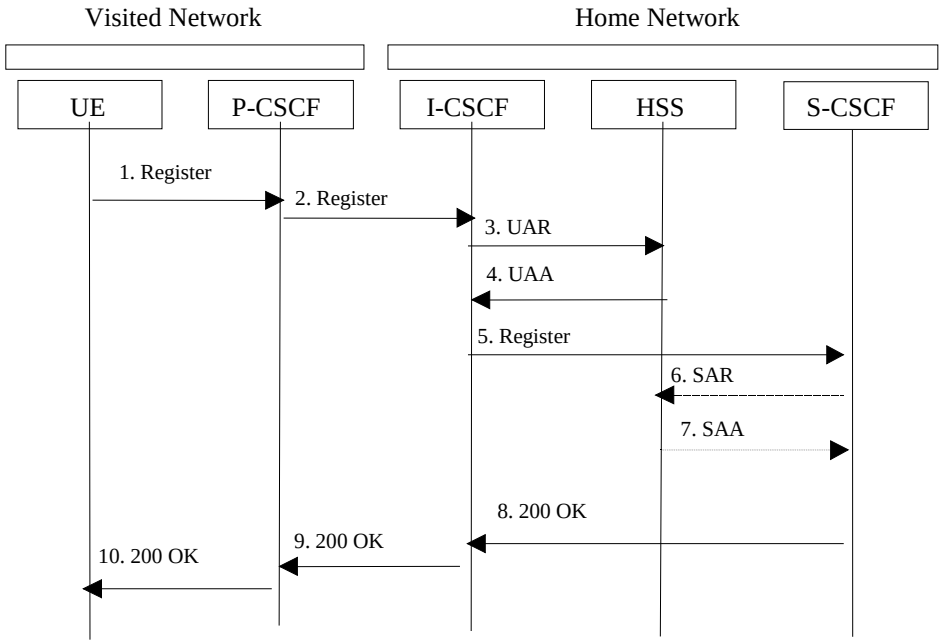


Figure A.4.2.1: Re-registration

A.4.3 UE initiated de-registration

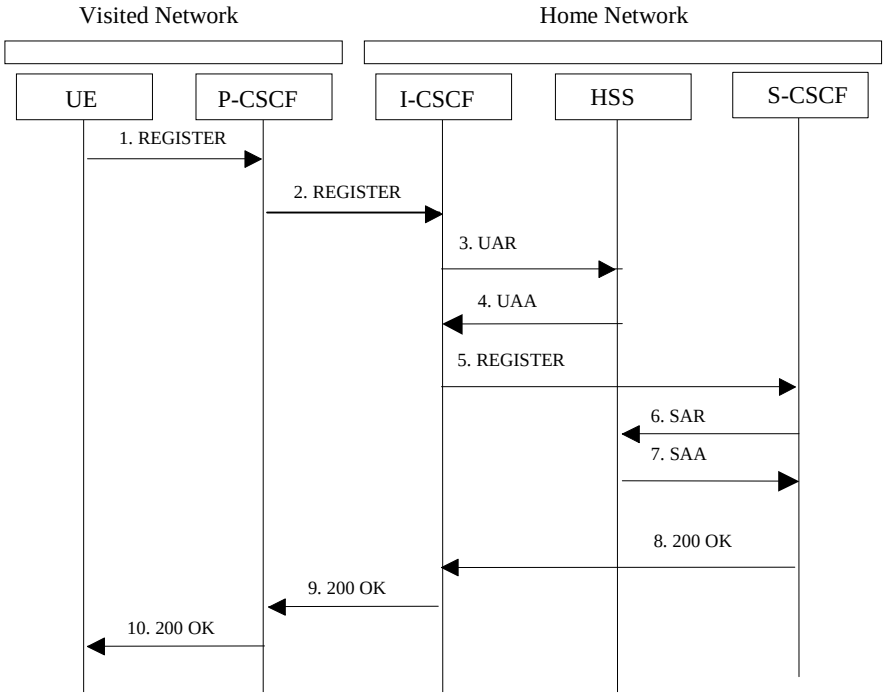


Figure A.4.3.1: UE initiated de-registration

A.4.4 Network initiated de-registration

A.4.4.1 Registration timeout

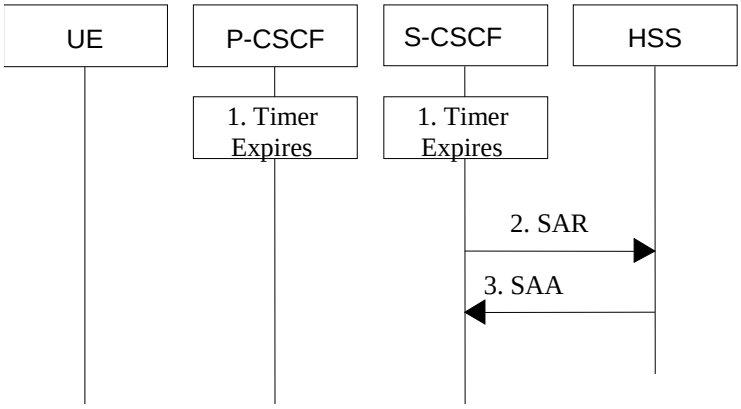


Figure A.4.4.1.1: Network initiated de-registration – registration timeout

A.4.4.2 Administrative de-registration

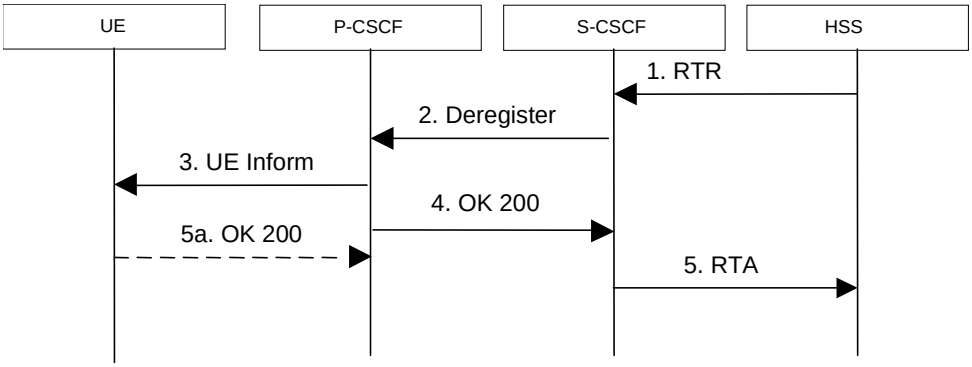


Figure A.4.4.2.1: Network initiated de-registration – administrative de-registration

A.4.4.3 De-registration initiated by service platform

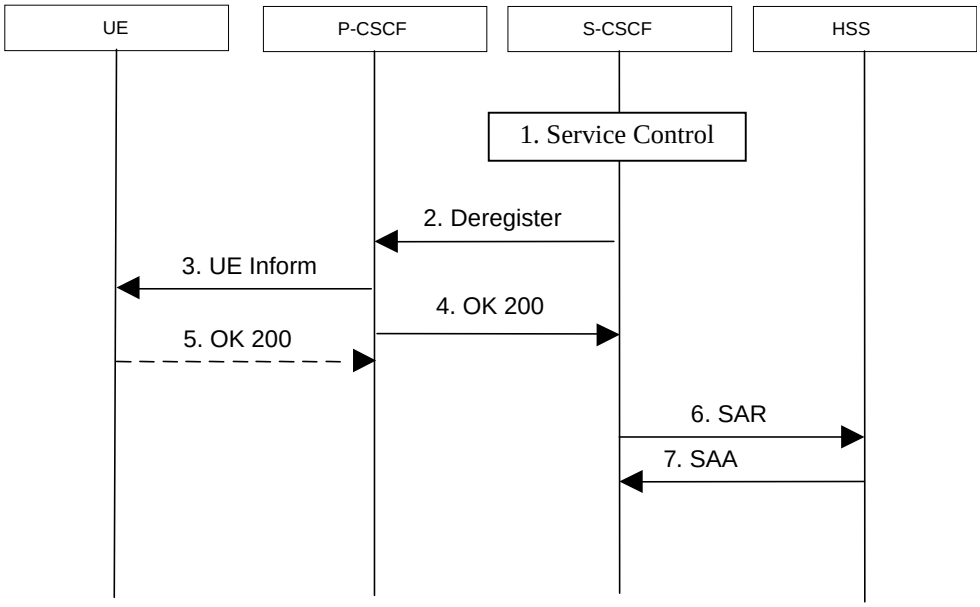


Figure A.4.4.3.1: Network initiated de-registration – initiated by service platform

A.4.5 UE Terminating SIP session set-up

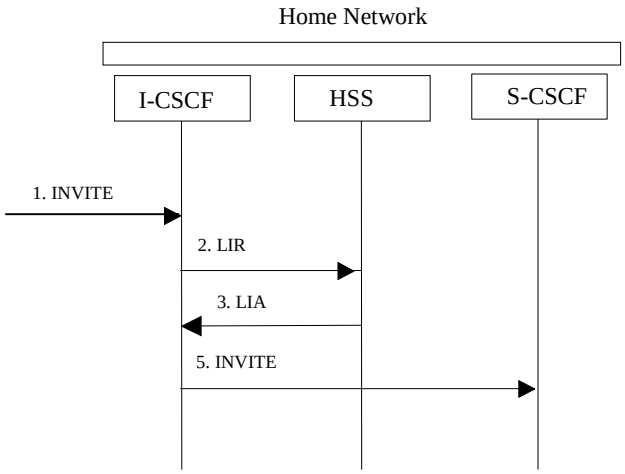


Figure A.4.5.1: UE Terminating SIP session set-up

A.4.6 Initiation of a session to a non-registered user

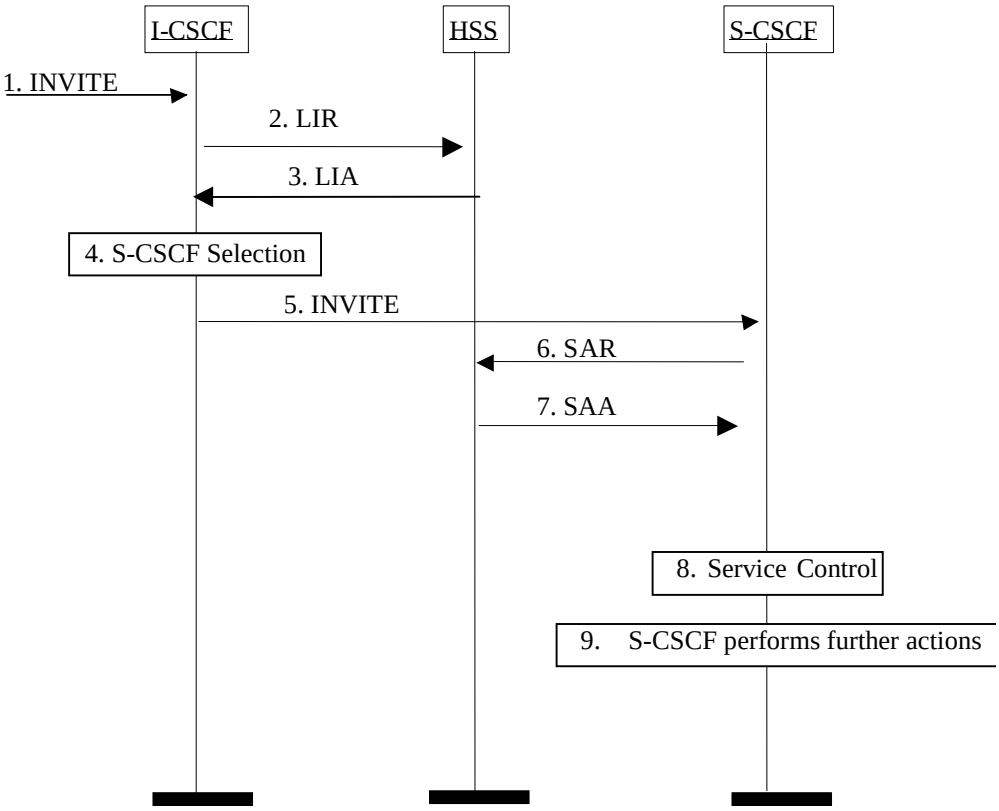


Figure A.4.6.1: Initiation of a session to a non-registered user

A.4.6a AS originating session on behalf of a non-registered user

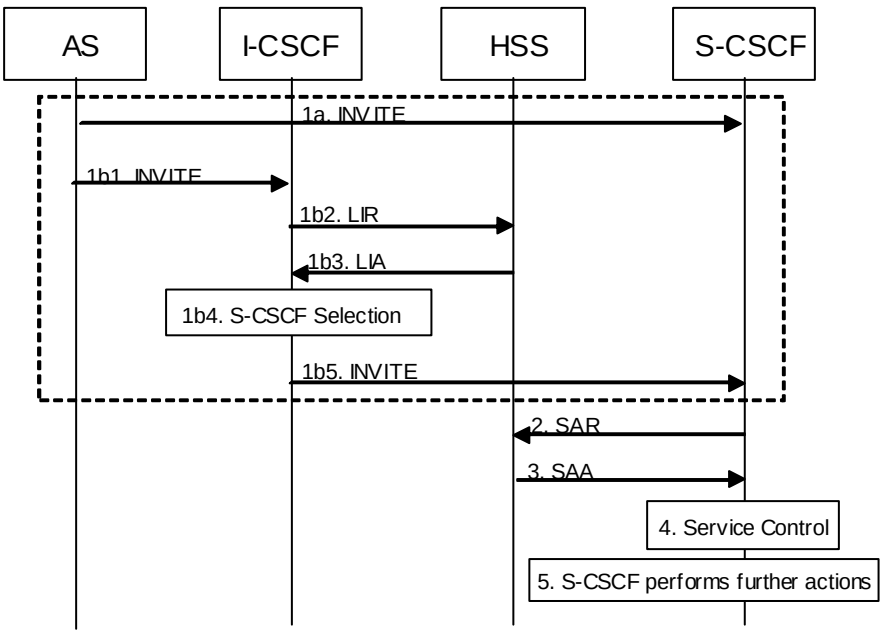


Figure A.4.6a.1: AS originating session on behalf of a non-registered user

A.4.7 User Profile update

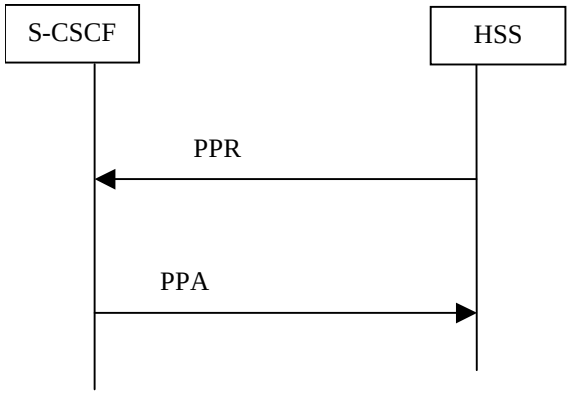


Figure A.4.7.1: User profile update

Annex B (informative): User profile UML model

The purpose of this UML model is to define in an abstract level the structure of the user profile downloaded over the Cx interface and describe the purpose of the different information classes included in the user profile.

B.1 General description

The following picture gives an outline of the UML model of the user profile, which is downloaded from HSS to S-CSCF:

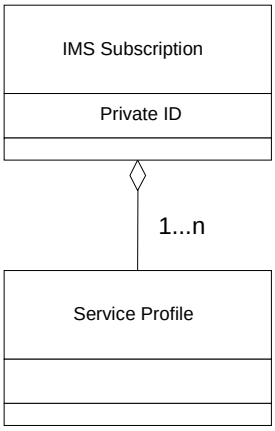


Figure B.1.1: User Profile

IMS Subscription class contains as a parameter the private user identity of the user in NAI format.

Each instance of the IMS Subscription class contains one or several instances of the class Service Profile.

B.2 Service profile

The following picture gives an outline of the UML model of the Service Profile class:

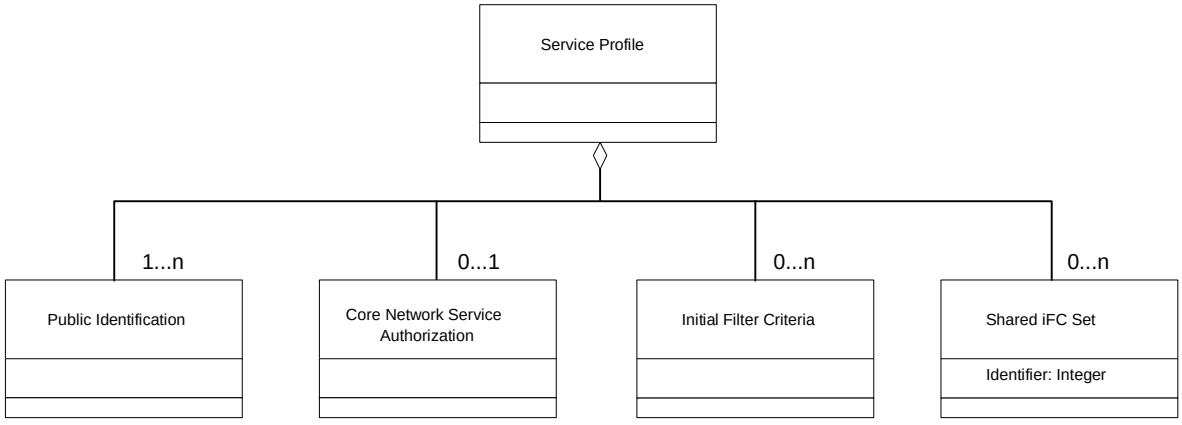


Figure B.2.1: Service Profile

Each instance of the Service Profile class consists of one or several instances of the class Public Identification. Public Identification class contains the Public Identities associated with that service profile. The information in the Core

Network Service Authorization, Initial Filter Criteria, and Shared iFC Set classes apply to all Public Identification instances, which are included in one Service profile class.

Each instance of the Service Profile class contains zero or one instance of the class Core Network Service Authorization. If no instance of the class Core Network Service Authorization is present, no filtering related to subscribed media or restriction on IMS Communication Service Identifiers applies in S-CSCF.

Each instance of the class Service Profile contains zero or several instances of the class Initial Filter Criteria.

Each instance of the class Service Profile contains zero or more instances of the class Shared iFC Set. A Shared iFC Set points to a set of Initial Filter Criteria locally administered and stored at the S-CSCF. Shared iFC Sets may be shared by several Service Profiles.

B.2.1 Public Identification

The following picture gives an outline of the UML model of Public Identification class:

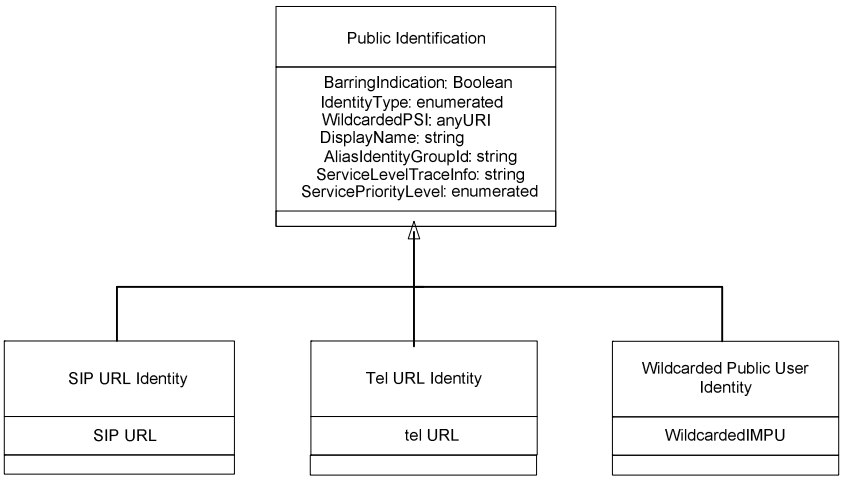


Figure B.2.1.1: Public Identification

Public Identification class can contain either SIP URL Identity, i.e. SIP URL, or Tel URL Identity class, i.e. tel URL, or Wildcarded Public User Identity, i.e. Wildcarded Public Service Identity or Wildcarded User Identity (see 3GPP TS 23.003 [17]),

The attribute BarringIndication is of type Boolean. If it is absent, or if it is present and set to FALSE, the S-CSCF shall not restrict the use of that public user identity in any IMS communications. If it is present and set to TRUE, the S-CSCF shall prevent that public identity from being used in any IMS communication except registrations and re-registrations, as specified in 3GPP TS 24.229 [8].

The attribute IdentityType indicates if the identity is a distinct Public User Identity, a distinct Public Service Identity, a Public Service Identity matching a Wildcarded Public Service Identity, a Public User Identity matching a Wildcarded Public User Identity, a Wildcarded Public Service Identity or a Wildcarded Public User Identity. If the identity type is not present, it is assumed to be a Public User Identity.

The attribute WildcardedPSI shall be present and contain the Wildcarded Public Service Identity that matched the Public Service Identity if the identity is a Public Service Identity matching a Wildcarded Public Service Identity. This Wildcarded Public Service identity shall be sent as stored in the HSS, that is, including the delimiter described in 3GPP TS 23.003 [17].

The attribute DisplayName allows a name to be associated with a Public Identity.

The attribute AliasIdentityGroupID indicates the alias group to which the Public User Identity belongs. If the "AliasInd" feature is supported, all Public User Identities shall have an AliasIdentityGroupID allocated. Within an IMS subscription Public User Identities that have the same AliasIdentityGroupID allocated shall not be in different implicit registration sets and shall share their service profile, and shall be regarded aliases of each other. If the "AliasInd" feature is not supported, all Public User Identities within an IMS subscription that are within the same implicit registration set and share their service profile shall be regarded aliases of each other.

The attribute WildcardedIMPU shall be present and contain the Wildcarded Public User Identity that matched the Public User Identity if the identity is a Public User Identity matching a Wildcarded Public User Identity. This Wildcarded Public User identity shall be sent as stored in the HSS, that is, including the delimiter described in 3GPP TS 23.003 [17].

The attribute ServiceLevelTraceInfo provides the Service Level Tracing Information that is related to the Public User Identity. If the ServiceLevelTraceInfo is present, service level tracing shall be enabled in the S-CSCF for the related Public User Identity according to the configuration data received. If the ServiceLevelTraceInfo is not present, service level tracing is disabled in the S-CSCF for the related Public User Identity.

The attribute ServicePriorityLevel provides the Priority Level allowed for the Public User Identity, which can be used by the S-CSCF and other network elements for Priority Service.

B.2.1A Core Network Service Authorization

The following picture gives an outline of the UML model of Core Network Service Authorization class:

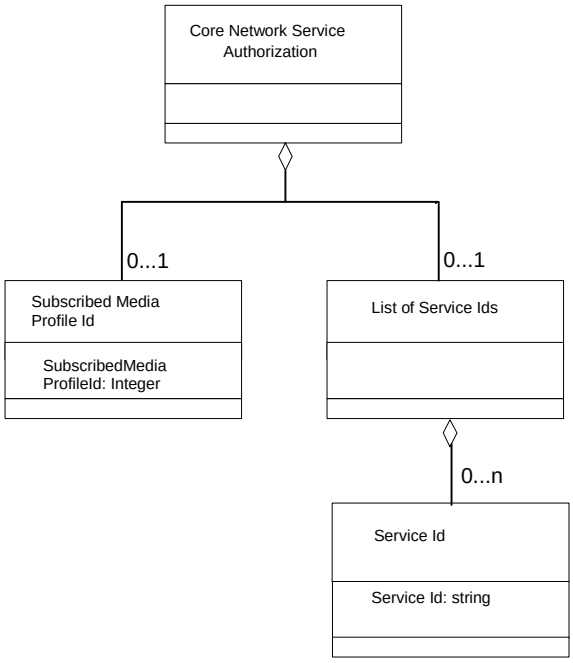


Figure B.2.1A.1: Core Network Service Authorization

Each instance of the Core Network Service Authorization class contains zero or one instance of the class Subscribed Media Profile Id. If no instance of the class Subscribed Media Profile Id is present, no filtering related to subscribed media applies in S-CSCF. The Subscribed Media Profile Id is of type Integer and identifies a media profile in the S-CSCF for the authorization of media parameters.

Each instance of the Core Network Service Authorization class contains zero or one instance of the class List of Service Ids. If no instance of the class List of Service Ids is present, no restriction on IMS Communication Service Identifiers related applies in S-CSCF. Each instance of the class List of Service Ids contains zero or more instances of the class Service Id. The Service Id is of type String and identifies an IMS Communication Service Identifier that the subscriber is authorized to use.

B.2.2 Initial Filter Criteria

The following picture gives an outline of the UML model of Initial Filter Criteria class:

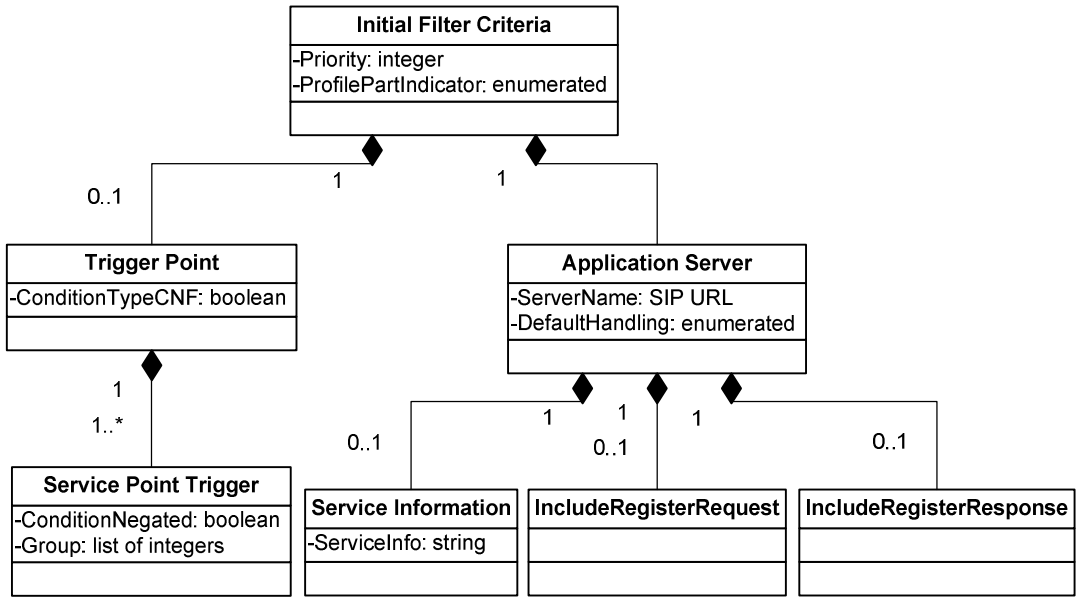


Figure B.2.2.1.1: Initial Filter Criteria

Each instance of the Initial Filter Criteria class is composed of zero or one instance of a Trigger Point class and one instance of an Application Server class. Priority indicates the priority of the Filter Criteria. The higher the Priority Number the lower the priority of the Filter Criteria is; i.e., a Filter Criteria with a higher value of Priority Number shall be assessed after the Filter Criteria with a smaller Priority Number have been assessed. The same priority shall not be assigned to more than one initial Filter Criterion.

ProfilePartIndicator attribute is an enumerated type, with possible values "REGISTERED and UNREGISTERED, indicating if the iFC is a part of the registered or unregistered user profile. If ProfilePartIndicator is missing from the iFC, the iFC is considered to be relevant to both the registered and unregistered parts of the user profile, i.e. belongs to the common part of the user profile.

Trigger Point class describes the trigger points that should be checked in order to find out if the indicated Application Server should be contacted or not. Each TriggerPoint is a boolean expression in Conjunctive or Disjunctive Normal form (CNF of DNF). The absence of Trigger Point instance will indicate an unconditional triggering to Application Server.

The attribute ConditionTypeCNF attribute defines how the set of SPTs are expressed, i.e. either an Ored set of ANDed sets of SPT statements or an ANDed set of Ored sets of statements. Individual SPT statements can also be negated. These combinations are termed, respectively, Disjunctive Normal Form (DNF) and Conjunctive Normal Form (CNF) for the SPT (see Annex C). Both DNF and CNF forms can be used. ConditionTypeCNF is a boolean that is TRUE when the Trigger Point associated with the FilterCriteria is a boolean expression in Conjunctive Normal Form (CNF) and FALSE if the Trigger Point is expressed in Disjunctive Normal Form (DNF) (see Annex C).

Each Trigger Point is composed by 1 to n instances of the class Service Point Trigger.

Application Server class defines the application server, which is contacted, if the trigger points are met. Server Name is the SIP URL of the application server to contact. Default Handling determines whether the dialog should be released if the Application Server could not be reached or not; it is of type enumerated and can take the values: SESSION_CONTINUED or SESSION_TERMINATED.

The Application Server class contains zero or one instance of the Service Information class, zero or one instance of the Include Register Request class and zero or one instance of the Include Register Response class. The Service Information class allows to download to S-CSCF information that is to be transferred transparently to an Application Server when the trigger points of a filter criterion are satisfied. ServiceInformation is a string conveying that information. See 3GPP TS 23.218 [7] for a description of the use of this information element. The Include Register Request class indicates to the S-CSCF that the incoming SIP REGISTER request is to be transferred to an Application Server when the trigger points of a filter criterion are satisfied. See 3GPP TS 23.218 [7] for a description of the use of this information element. The Include Register Response class indicates to the S-CSCF that the final SIP response to the incoming SIP REGISTER request is to be transferred to an Application Server when the trigger points of a filter criterion are satisfied. See 3GPP TS 23.218 [7] for a description of the use of this information element.

B.2.3 Service Point Trigger

The following picture gives an outline of the UML model of Service Point Trigger class:

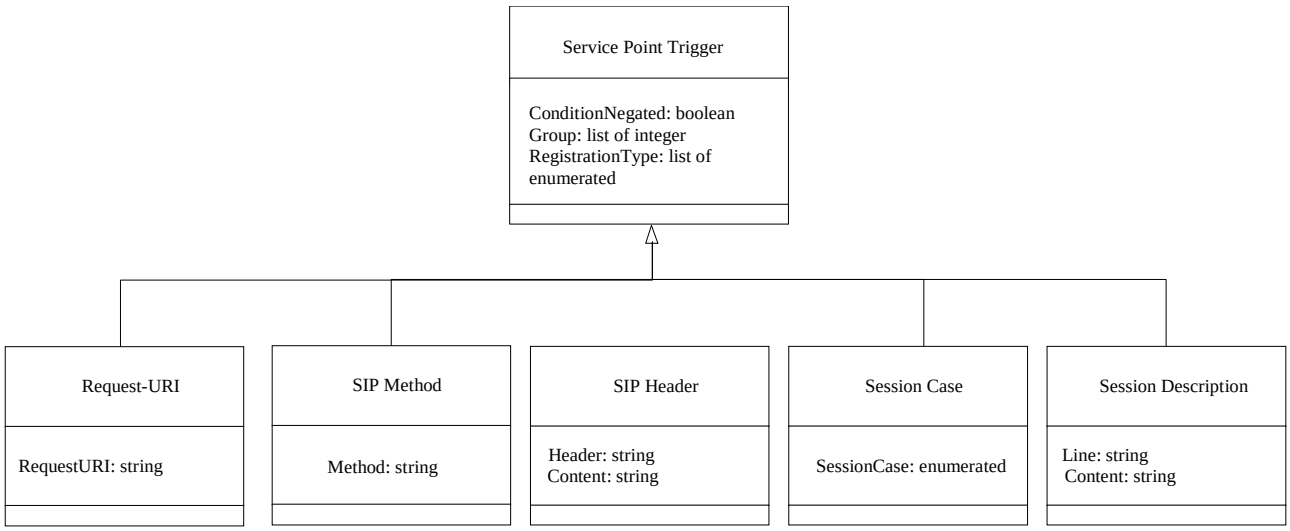


Figure B.2.3.1: Service Point Trigger

The attribute Group of the class Service Point Trigger allows the grouping of SPTs that will configure the sub-expressions inside a CNF or DNF expression. For instance, in the following CNF expression (A+B).(C+D), A+B and C+D would correspond to different groups.

In CNF, the attribute Group identifies the ORed sets of SPT instances. If the SPT belongs to different ORed sets, SPT can have more than one Group values assigned. At least one Group must be assigned for each SPT.

In DNF, the attribute Group identifies the ANDed sets of SPT instances. If the SPT belongs to different ANDed sets, SPT can have more than one Group values assigned. At least one Group must be assigned for each SPI.

The attribute ConditionNegated of the class Service Point Trigger defines whether the individual SPT instance is negated (i.e. NOT logical expression).

The attribute RegistrationType of the class Service Point Trigger is relevant only to the SIP Method SPT with a value of "REGISTER" and its' support is optional in the HSS and in the S-CSCF. The RegistrationType may contain a list of values that define whether the SPT matches to REGISTER messages that are related to initial registrations, re-registrations, and/or de-registrations. If RegistrationTypes are given, the SIP Method SPT with a value of "REGISTER" shall match if any of the RegistrationTypes match and the S-CSCF supports the RegistrationType attribute. If the SIP Method SPT contains value "REGISTER", and no RegistrationType is given, or if the S-CSCF does not support the RegistrationType attribute, the SIP Method SPT matches to all REGISTER messages. The attribute RegistrationType may be discarded if it is present in an SPT other than SIP Method with value "REGISTER".

Request-URI class defines SPT for the Request-URI. Request-URI contains attribute RequestURI.

SIP Method class defines SPT for the SIP method. SIP Method contains attribute Method which holds the name of any SIP method.

SIP Header class defines SPT for the presence or absence of any SIP header or for the content of any SIP header. SIP Header contains attribute Header which identifies the SIP Header, which is the SPT, and the Content attribute defines the value of the SIP Header if required.

The absence of the Content attribute and ConditionNegated = TRUE indicates that the SPT is the absence of a determined SIP header.

Session Case class represents an enumerated type, with possible values "Originating", "Terminating_Registered", "Terminating_Unregistered", "Originating_Unregistered", "Originating_CDIV" indicating whether the filter should be

used by the S-CSCF handling the Originating, Terminating for a registered end user, Terminating for an unregistered end user, Originating for an unregistered end user, or Originating after Call Diversion services.

Session Description Information class defines SPT for the content of any SDP field within the body of a SIP Method. The Line attribute identifies the line inside the session description. Content is a string defining the content of the line identified by Line.

Annex C (informative): Conjunctive and Disjunctive Normal Form

A Trigger Point expression is constructed out of atomic expressions (i.e. Service Point Trigger) linked by Boolean operators AND, OR and NOT. Any logical expression constructed in that way can be transformed to forms called Conjunctive Normal Form (CNF) and Disjunctive Normal Form (DNF).

A Boolean expression is said to be in Conjunctive Normal Form if it is expressed as a conjunction of disjunctions of literals (positive or negative atoms), i.e. as an AND of clauses, each of which is the OR of one of more atomic expressions.

Taking as an example the following trigger:

Method = "INVITE" OR Method = "MESSAGE" OR (Method="SUBSCRIBE" AND NOT Header = "from" Content = "joe")

The trigger can be split into the following atomic expressions:

Method="INVITE"

Method="MESSAGE"

Method="SUBSCRIBE"

NOT header="from" Content ="joe"

Grouping the atomic expressions, the CNF expression equivalent to the previous example looks like:

(Method="INVITE" OR Method = "MESSAGE" OR Method="SUBSCRIBE") AND (Method="INVITE" OR Method = "MESSAGE" OR (NOT Header = "from" Content = "joe"))

This result in two "OR" groups linked by "AND" (CNF):

(Method="INVITE" OR Method = "MESSAGE" OR Method="SUBSCRIBE")

(Method="INVITE" OR Method = "MESSAGE" OR (NOT Header = "from" Content = "joe"))

The XML representation of the trigger is:

```
<?xml version="1.0" encoding="UTF-8"?>
<IMSSubscription xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="CxDataType.xsd">
        <PrivateID>IMPI1@homedomain.com</PrivateID>
        <ServiceProfile>
                <PublicIdentity>
                        <BarringIndication>1</BarringIndication>
                        <Identity> sip:IMPU1@homedomain.com </Identity>
                </PublicIdentity>
                <PublicIdentity>
                        <Identity> sip:IMPU2@homedomain.com </Identity>
                </PublicIdentity>
                <InitialFilterCriteria>
                        <Priority>0</Priority>
                        <TriggerPoint>
                                <ConditionTypeCNF>1</ConditionTypeCNF>
                                <SPT>
                                        <ConditionNegated>0</ConditionNegated>
                                        <Group>0</Group>
                                        <Method>INVITE</Method>
```

```
                                </SPT>
                                <SPT>
                                        <ConditionNegated>0</ConditionNegated>
                                        <Group>0</Group>
                                        <Method>MESSAGE</Method>
                                </SPT>
                                <SPT>
                                        <ConditionNegated>0</ConditionNegated>
                                        <Group>0</Group>
                                        <Method>SUBSCRIBE</Method>
                                </SPT>
                                <SPT>
                                        <ConditionNegated>0</ConditionNegated>
                                        <Group>1</Group>
                                        <Method>INVITE</Method>
                                </SPT>
                                <SPT>
                                        <ConditionNegated>0</ConditionNegated>
                                        <Group>1</Group>
                                        <Method>MESSAGE</Method>
                                </SPT>

                                <SPT>
                                        <ConditionNegated>1</ConditionNegated>
                                        <Group>1</Group>
                                        <SIPHeader>
                                                <Header>From</Header>
                                                <Content>"joe"</Content>
                                        </SIPHeader>
                                </SPT>
                        </TriggerPoint>
                        <ApplicationServer>
                                <ServerName>sip:AS1@homedomain.com</ServerName>
                                <DefaultHandling>0</DefaultHandling>
                        </ApplicationServer>
                </InitialFilterCriteria>
        </ServiceProfile>
</IMSSubscription>
```

A Boolean expression is said to be in Disjunctive Normal Form if it is expressed as a disjunction of conjunctions of literals (positive or negative atoms), i.e. as an OR of clauses, each of which is the AND of one of more atomic expressions.

The previous example is already in DNF, composed by the following groups:

Method="INVITE"

Method="MESSAGE"

Method="SUBSCRIBE" AND (NOT header="from" Content ="joe")

The XML representation of the trigger is:

```
<?xml version="1.0" encoding="UTF-8"?>
<IMSSubscription xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="CxDataType.xsd">
        <PrivateID>IMPI1@homedomain.com</PrivateID>
        <ServiceProfile>
                <PublicIdentity>
                        <BarringIndication>1</BarringIndication>
                        <Identity> sip:IMPU1@homedomain.com </Identity>
                </PublicIdentity>
```

```
                <PublicIdentity>
                        <Identity> sip:IMPU2@homedomain.com </Identity>
                </PublicIdentity>
                <InitialFilterCriteria>
                        <Priority>0</Priority>
                        <TriggerPoint>
                                <ConditionTypeCNF>0</ConditionTypeCNF>
                                <SPT>
                                        <ConditionNegated>0</ConditionNegated>
                                        <Group>0</Group>
                                        <Method>INVITE</Method>
                                </SPT>
                                <SPT>
                                        <ConditionNegated>0</ConditionNegated>
                                        <Group>1</Group>
                                        <Method>MESSAGE</Method>
                                </SPT>
                                <SPT>
                                        <ConditionNegated>0</ConditionNegated>
                                        <Group>2</Group>
                                        <Method>SUBSCRIBE</Method>
                                </SPT>
                                <SPT>
                                        <ConditionNegated>1</ConditionNegated>
                                        <Group>2</Group>
                                        <SIPHeader>
                                                <Header>From</Header>
                                                <Content>"joe"</Content>
                                        </SIPHeader>
                                </SPT>
                        </TriggerPoint>
                        <ApplicationServer>
                                <ServerName>sip:AS1@homedomain.com</ServerName>
                                <DefaultHandling index="0">0</DefaultHandling>
                        </ApplicationServer>
                </InitialFilterCriteria>
        </ServiceProfile>
</IMSSubscription>
```

Annex D (informative): High-level format for the User Profile

The way the information shall be transferred through the Cx interface can be seen from a high-level point of view in the following picture:

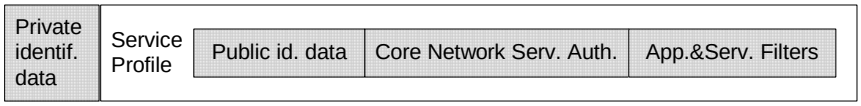


Figure D.1: Example of in-line format of user profile

If more than one service profile is created, for example to assign a different set of filters to public identifiers 1 and 2 and public identity 3, the information shall be packaged in the following way:



Figure D.2: Example of in-line format of user profile

Annex E (normative): XML schema for the Cx interface user profile

The file CxDataType_Rel8.xsd, attached to this specification, contains the XML schema for the user profile that is sent over the Cx interface. The user profile XML schema defines that are used in the user profile XML. The data that is allowed to be sent in the user profile may vary depending on the features supported by the Diameter end points, see 3GPP TS 29.229 [5]. The user profile XML schema file is intended to be used by an XML parser. The version of the Cx application sending the user profile XML shall be the same as the version of the sent user profile XML and thus it implies the version of the user profile XML schema to be used to validate it.

Table E.1 describes the data types and the dependencies among them that configure the user profile XML schema.

Table E.1: XML schema for the Cx interface user profile: simple data types

Data type	Tag	Base type	Comments
tPriority	Priority	integer	>= 0
tProfilePartIndicator	ProfilePartIndicator	enumerated	Possible values: 0 (REGISTERED) 1 (UNREGISTERED)
tSharedIFCSetID	SharedIFCSetID	integer	>= 0
tGroupID	Group	integer	>= 0
tRegistrationType	RegistrationType	enumerated	Possible values: 0 (INITIAL_REGISTRATION) 1 (RE-REGISTRATION) 2 (DE-REGISTRATION)
tDefaultHandling	DefaultHandling	enumerated	Possible values: 0 (SESSION_CONTINUED) 1 (SESSION_TERMINATED)
tDirectionOfRequest	SessionCase	enumerated	Possible values: 0 (ORIGINATING_SESSION) 1 TERMINATING_REGISTERED 2 (TERMINATING_UNREGISTERED) 3 (ORIGINATING_UNREGISTERED) 4 (ORIGINATING_CDIV)
tPrivateID	PrivateID	anyURI	Syntax described in IETF RFC 2486 [14]
tSIP_URL	Identity	anyURI	Syntax described in IETF RFC 3261 [11]
tTEL_URL	Identity	anyURI	Syntax described in IETF RFC 3966 [15]
tIdentity	Identity	(union)	Union of tSIP_URL, and tTEL_URL and tWildcardedIMPU
tIdentityType	IdentityType	enumerated	Possible values: 0 (PUBLIC_USER_IDENTITY) 1 (DISTINCT_PSI) 2 (WILDCARDED_PSI) 3 (WILDCARDED_IMPU) (See Note 1) 4 (IMPU_WILDCARD) (See Note 1)
tServiceInfo	ServiceInfo	string	
tString	RequestURI, Method, Header, Content, Line	string	
tBool	ConditionTypeCNF, ConditionNegated, BarringIndication	boolean	Possible values: 0 (false) 1 (true)
tSubscribedMediaProfileId	SubscribedMediaProfileId	integer	>=0
tDisplayName	DisplayName	string	
tAliasIdentityGroupID	AliasIdentityGroupID	string	
tServiceLevelTraceInfo	ServiceLevelTraceInfo	string	Syntax described in clause 14 within IETF draft-dawes-sipping-debug [20]
tServicePriorityLevel	ServicePriorityLevel	enumerated	Possible values: 0 (Highest priority) 1 2 3 4 (Lowest priority)
NOTE 1: IMPU _WILDCARD indicates that the content of the identity in the “Identity” tag is a Wildcarded Public User Identity, while WILDCARDED_IMPU indicates that it is a specific Public User Identity matching a Wildcarded Public User Identity.			

Table E.2: XML schema for the Cx interface user profile: complex data types

Data type	Tag	Compound of		
		Tag	Type	Cardinality
tIMSSubscription	IMSSubscription	PrivateID	tPrivateID	1
		ServiceProfile	tServiceProfile	(1 to n)
tServiceProfile	ServiceProfile	PublicIdentity	tPublicIdentity	(1 to n)
		CoreNetworkServicesAuthorization	CoreNetworkServicesAuthorization	(0 to 1)
		InitialFilterCriteria	tInitialFilterCriteria	(0 to n)
		Extension	tServiceProfileExtension	(0 to 1)
tServiceProfileExtension	Extension	SharedIFCSetID	tSharedIFCSetID	(0 to n)
tCoreNetworkServicesAuthorization	CoreNetworkServicesAuthorization	SubscribedMediaProfileId	tSubscribedMediaProfileId	(0 to 1)
		Extension	tCNServicesAuthorizationExtension	(0 to 1)
tPublicIdentity	PublicIdentity	BarringIndication	tBool	(0 to 1)
		Identity	tIdentity	1
		Extension	tPublicIdentityExtension	(0 to 1)
tInitialFilterCriteria	InitialFilterCriteria	Priority	tPriority	1
		TriggerPoint	tTrigger	(0 to 1)
		ApplicationServer	tApplicationServer	1
		ProfilePartIndicator	tProfilePartIndicator	(0 to 1)
tTrigger	TriggerPoint	ConditionTypeCNF	tBool	1
		SPT	tSePoTri	(1 to n)
tSePoTri	SPT	ConditionNegated	tBool	(0 to 1)
		Group	tGroupID	(1 to n
		Choice of: RequestURI	tString	1
		Choice of: Method	tString	1
		Choice of: SIPHeader	tHeader	1
		Choice of: SessionCase	tDirectionOfRequest	1
		Choice of: SessionDescription	tSessionDescription	1
		Extension	tSePoTriExtension	(0 to 1)
tSePoTriExtension	Extension	RegistrationType	tRegistrationType	(0 to 2)
tHeader	SIPHeader	Header	tString	1
		Content	tString	(0 to 1)
tSessionDescription	SessionDescription	Line	tString	1
		Content	tString	(0 to 1)
tApplicationServer	ApplicationServer	ServerName	tSIP_URL	1
		DefaultHandling	tDefaultHandling	(0 to 1)
		ServiceInfo	tServiceInfo	(0 to 1)
		Extension	tApplicationServerExtension	(0 to 1)
tApplicationServerExtension	Extension	IncludeRegisterRequest	tIncludeRegisterRequest	(0 to 1)
		IncludeRegisterResponse	tIncludeRegisterResponse	(0 to 1)
tIncludeRegisterRequest	IncludeRegisterRequest	(NOTE 2)	(NOTE 2)	(0 to 1)
tIncludeRegisterResponse	tIncludeRegisterResponse	(NOTE 2)	(NOTE 2)	(0 to 1)
tPublicIdentityExtension	Extension	IdentityType	tIdentityType	(0 to 1)
		WildcardedPSI	anyURI (NOTE 3)	(0 to 1)
		Extension	tPublicIdentityExtension2	(0 to 1)
tPublicIdentityExtension2	Extension	DisplayName	tDisplayName	(0 to 1)
		AliasIdentityGroupID	tAliasIdentityGroupID	(0 to 1)
		Extension	tPublicIdentityExtension3	(0 to 1)
tPublicIdentityExtension3	Extension	WildcardedIMPU	anyURI (NOTE 3)	(0 to 1)
		ServiceLevelTraceInfo	tServiceLevelTraceInfo	(0 to 1)
		ServicePriorityLevel	ServicePriorityLevel	(0 to 1)
tCNServicesAuthorizationExtension	Extension	ListOfServiceIds	tListOfServiceIds	(0 to 1)
tListOfServiceIds	ListOfServiceIds	ServiceId	tString	(0 to n)

NOTE 1: "n" shall be interpreted as non-bounded.
NOTE 2: empty cells shall be interpreted as complex XML elements without defined content.
NOTE 3: the syntax of Wildcarded Public User Identity and Wildcarded Service Identity shall be as described in 3GPP TS 23.003 [17]

Annex F (normative): Definition of parameters for service point trigger matching

Table F.1 defines the parameters that are transported in the user profile XML.

Table F.1: Definition of parameters in the user profile XML

Tag	Description
SIPHeader	A SIP Header SPT shall be evaluated separately against each header instance within the SIP message. The SIP Header SPT matches if at least one header occurrence matches the SPT.
Header (of SIPHeader)	Header tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in IEEE 1003.1-2004 Part 1 [13]. The regular expression shall be matched against the header-name of the SIP header. For definition of header and header-name, see IETF RFC 3261 [11]. Before matching the header-name to the pattern, all SWSs shall be removed from the header-name and all LWSs in the header-name shall be reduced to a single white space character (SP). For definition of SWS and LWS, see IETF RFC 3261 [11].
Content (of SIPHeader)	Content tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in IEEE 1003.1-2004 Part 1 [13]. The regular expression shall be matched against the header-value of the SIP header. For definition of header and header-value, see IETF RFC 3261 [11]. If the SIP header contains several header-values in a comma-separated list, each of the header-value shall be matched against the pattern for the Content separately. Before matching the header-value to the pattern, all SWSs shall be removed from the header-value and all LWSs in the header-value shall be reduced to a single white space character (SP). For definition of SWS and LWS, see IETF RFC 3261 [11].
SessionDescription	A Session Description SPT shall be evaluated separately against each SDP field instance within the SIP message. The Session Description SPT matches if at least one field occurrence matches the SPT.
Line (of SessionDescription)	Line tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in IEEE 1003.1-2004 Part 1 [13]. The regular expression shall be matched against the type of the field inside the session description. For definition of type, see chapter 6 in IETF RFC 4566 [12].
Content (of SessionDescription)	Content tag shall include a regular expression in a form of Extended Regular Expressions (ERE) as defined in chapter 9 in IEEE 1003.1-2004 Part 1 [13]. The regular expression shall be matched against the value of the field inside the session description. For definition of value, see chapter 6 in IETF RFC 4566 [12].

Annex G (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
Jun 2002	CN#16	NP-020264			Version 2.0.0 approved at CN#16	2.0.0	5.0.0
Sep 2002	CN#17	NP-020449	001	2	Clarification of implicit registration	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	002	1	Clarification of user registration status query	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	003	1	Clarification of HSS initiated update of user profile	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	004	2	Clarification of MAR command	5.0.0	5.1.0
Sep 2002	CN#17	NP-020449	005	1	Conditionality of the SIP-Auth-Data-Item in MAA command	5.0.0	5.1.0
Dec 2002	CN#18	NP-020587	008	2	Rejection of registration of a Temporary Public Identity without active implicit registration	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	010	-	Removal of upper bounds in Cx i/f user profile	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	011	-	S-CSCF Assignment	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	012	-	NAS-Session-Key AVPs in MAA command	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	013	1	Correction to detailed behaviour of user registration status query	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	014	1	Removing the DDF dependencies from Cx interface	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	015	1	Clarification of SERVER_CHANGE de-registration reason code	5.1.0	5.2.0
Dec 2002	CN#18	NP-020589	016	1	Clarification of User-Authorization-Type AVP usage within the UAR	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	017	1	Correction to HSS initiated update of user profile	5.1.0	5.2.0
Dec 2002	CN#18	NP-020588	019	-	Correction in charging information	5.1.0	5.2.0
Dec 2002	CN#18	NP-020590	020	1	Error handling in S-CSCF when receiving too much data	5.1.0	5.2.0
Dec 2002	CN#18	NP-020587	021	1	Re-allocation of S-CSCF	5.1.0	5.2.0
Dec 2002	CN#18	NP-020591	022	-	Correction of the SPI	5.1.0	5.2.0
Mar 2003	CN#19	NP-030101	025	1	Clarification of service profile download at service profile modification	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	028	-	Filter ID field removal in InitialFilterCriteria class	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	030	1	Clarification of IMPU barring handling	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	032	1	The default public user identity in the Server-Assignment-Answer	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	034	2	Corrections to service profile	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	037	3	Handling of non supported data in the S-CSCF when the profile is being updated	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	024	1	Clarification of the HSS behaviour in REGISTRATION and DE_REGISTRATION procedures at IMPU checking time.	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	027	-	Deletion of Annex F	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	029	-	Clarification of User-Authorization-Type AVP usage within UAR	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	031	1	Update TS 29.228 after Diameter has become RFC	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	033	1	Replacement of the NAS-Session-Key AVP	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	035	2	Clarification on Re-allocation of S-CSCF	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	038	1	Change of SPI to SPT	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	040	1	Definition of the Subscribed Media Profile Identifier	5.2.0	5.3.0
Mar 2003	CN#19	NP-030101	026	-	Error in definition of Service Point of Interest class	5.2.0	5.3.0
Jun 2003	CN#20	NP-030215	043	-	Correct use of the Result-Code AVP	5.3.0	5.4.0
Jun 2003	CN#20	NP-030215	044	1	Conditionality of User-Name AVP in Server-Assignment-Answer	5.3.0	5.4.0
Jun 2003	CN#20	NP-030215	045	2	Corrections to the base 64 encoding examples	5.3.0	5.4.0
Jun 2003	CN#20	NP-030215	046	1	Deregistration of implicitly registered public user identities	5.3.0	5.4.0
Jun 2003	CN#20	NP-030215	047	-	Clarification on the Server-Assignment-Type NO_ASSIGNMENT	5.3.0	5.4.0
Jun 2003	CN#20	NP-030215	048	1	Incorrect use of result-code	5.3.0	5.4.0
Jun 2003	CN#20	NP-030215	049	1	Misalignment in the Public-User-Identity IE	5.3.0	5.4.0
Jun 2003	CN#20	NP-030215	050	1	Duplicated Destination-Host AVP within MAR command code	5.3.0	5.4.0
Sep 2003	CN#21	NP-030383	042	3	Error in S-CSCF Assignment Type	5.4.0	5.5.0
Sep 2003	CN#21	NP-030383	051	2	Mistakes in the XML schema of 29.228-540	5.4.0	5.5.0
Sep 2003	CN#21	NP-030383	055	1	Extensibility of the public identity structure in the XML schema	5.4.0	5.5.0
Sep 2003	CN#21	NP-030394	041	2	Introduction of Presence Stage 3 (Px) to the Cx interface	5.5.0	6.0.0
Sep 2003	CN#21	NP-030394	052	-	Sharing public identities across multiple UEs	5.5.0	6.0.0
Dec 2003	CN#22	NP-030585	057	3	Conditions for inclusion of Charging Information	6.0.0	6.1.0
Dec 2003	CN#22	NP-030500	060	1	MAR in synchronisation failure case	6.0.0	6.1.0
Dec 2003	CN#22	NP-030500	061	1	The S-CSCF name needs to be checked always in MAR	6.0.0	6.1.0
Dec 2003	CN#22	NP-030500	063	-	Conditional AVPs in answer commands	6.0.0	6.1.0
Dec 2003	CN#22	NP-030500	065	1	Server-Assignment-Request	6.0.0	6.1.0
Dec 2003	CN#22	NP-030500	067	-	Determination of User-Authorization-Type AVP based on registration expiration	6.0.0	6.1.0
Dec 2003	CN#22	NP-030500	069	2	Not registered state after deregistration with S-CSCF deleted at the HSS	6.0.0	6.1.0
Dec 2003	CN#22	NP-030500	071	-	The extensibility of the XML schema	6.0.0	6.1.0
Dec 2003	CN#22			-	Reference [9] updated	6.0.0	6.1.0

Mar 2004	CN#23	NP-040046	077	1	Clarification on S-CSCF-Name comparison	6.1.0	6.2.0
Mar 2004	CN#23	NP-040055	081	-	Error for missing identification in SAR command	6.1.0	6.2.0
Mar 2004	CN#23	NP-040046	085	1	Conditions for inclusion of Public Identity in SAR	6.1.0	6.2.0
Mar 2004	CN#23	NP-040046	087	1	Correction to sending the Charging-Information AVP	6.1.0	6.2.0
Mar 2004	CN#23	NP-040046	089	-	Correction to User-Authorization-Answer	6.1.0	6.2.0
Mar 2004	CN#23	NP-040046	091	-	Default handling of error cases during IMS registration	6.1.0	6.2.0
Jun 2004	CN#24	NP-040215	097	2	Update of the charging addresses from HSS	6.2.0	6.3.0
Jun 2004	CN#24	NP-040215	095	1	Content of the User Profile	6.2.0	6.3.0
Jun 2004	CN#24	NP-040215	099	-	Correction of SessionCase attribute ambiguity	6.2.0	6.3.0
Sep 2004	CN#25	NP-040416	109	1	LIR and services related to unregistered state	6.3.0	6.4.0
Sep 2004	CN#25	NP-040401	121	2	Triggering initial REGISTER messages	6.3.0	6.4.0
Sep 2004	CN#25	NP-040401	118	1	XML versioning	6.3.0	6.4.0
Sep 2004	CN#25	NP-040401	122	1	Optimization of User Profile Download	6.3.0	6.4.0
Sep 2004	CN#25	NP-040396	124	2	Simplification of the User Profile Split concept	6.3.0	6.4.0
Sep 2004	CN#25	NP-040416	120	3	Use of regular expressions	6.3.0	6.4.0
Dec 2004	CN#26	NP-040523	138	1	HSS initiated deregistration with "not registered" registration state	6.4.0	6.5.0
Dec 2004	CN#26	NP-040530	140	1	HSS initiated deregistration with user profile removal for permanent termination	6.4.0	6.5.0
Dec 2004	CN#26	NP-040523	142	2	HSS initiated deregistration using the network initiated de-registration procedure	6.4.0	6.5.0
Dec 2004	CN#26	NP-040530	146	1	Clarification of R6 authentication scheme	6.4.0	6.5.0
Dec 2004	CN#26	NP-040523	150	-	Regular Expressions	6.4.0	6.5.0
Dec 2004	CN#26	NP-040530	155	-	Correction to XML Root Element	6.4.0	6.5.0
Dec 2004	CN#26	NP-040530	156	1	Modification of User-Data-Already-Available in SAR command.	6.4.0	6.5.0
Dec 2004	CN#26	NP-040523	159	2	Handling of Information Element marked as (M), (C) or (O)	6.4.0	6.5.0
Mar 2005	CN#27	NP-050030	166	-	Avoiding undesired deregistration	6.5.0	6.6.0
Mar 2005	CN#27	NP-050030	168	1	Correction to authentication procedures in not registered case	6.5.0	6.6.0
Mar 2005	CN#27	NP-050037	170	3	Clarification of behaviour for Shared Public User Identities	6.5.0	6.6.0
Mar 2005	CN#27	NP-050037	172	-	Distribution of Cipher Key and Integrity Key	6.5.0	6.6.0
Apr 2005					Editorial correction on figure figure A.4.1.1 and on clauses: 6.1.4.1, 6.2.2, B.2.1 and 6.2.1.1	6.6.0	6.6.1
Jun 2005	CT#28	CP-050086	181	-	TEL-URI reference correction	6.6.1	6.7.0
Jun 2005	CT#28	CP-050086	183	-	Clarification on Server Capabilities	6.6.1	6.7.0
Jun 2005	CT#28	CP-050086	185	-	Incorrect Implementation of CR172	6.6.1	6.7.0
Jun 2005	CT#28	CP-050081	188	1	Clarification of the content of SIP-Authentication-Context	6.6.1	6.7.0
Jun 2005	CT#28	CP-050086	192	-	Syntax correction for XML	6.6.1	6.7.0
Sep 2005	CT#29	CP-050422	196	-	Authentication Registration with synchronization failure, Data requested from HSS	6.7.0	6.8.0
Sep 2005	CT#29	CP-050296	200		Correction to XML Schema for SharedIFCSet	6.7.0	6.8.0
Sep 2005	CT#29	CP-050440	202	2	Private identities on the Cx	6.7.0	6.8.0
Sep 2005	CT#29	CP-050282	204	1	Charging-Information correction	6.7.0	6.8.0
Sep 2005	CT#29	CP-050296	207	1	Corrections to UAR and LIR for shared public identities	6.7.0	6.8.0
Sep 2005	CT#29	CP-050422	208	1	Behaviour of the Implicit Registration Set for the Unregistered state	6.7.0	6.8.0
Sep 2005	CT#29	CP-050296	210	-	Change of stage 2 reference from Release 5 to Release 6	6.7.0	6.8.0
Sep 2005	CT#29	CP-050294	211	-	PSI Activation	6.7.0	6.8.0
Sep 2005	CT#29	CP-050271	213	2	Removal of redundant restrictions for one Public User Identity in SAR	6.7.0	6.8.0
Sep 2005	CT#29	CP-050296	216	-	Error code clean up	6.7.0	6.8.0
Sep 2005	CT#29	CP-050296	217	1	Clarification of User Profile update	6.7.0	6.8.0
Dec 2005	CT#30	CP-050604	198	5	XML syntax correction	6.8.0	6.9.0
Dec 2005	CT#30	CP-050611	220	1	PSI impacts on the Cx Interface	6.8.0	6.9.0
Dec 2005	CT#30	CP-050611	221	3	Routing for PSIs Matching a Wildcarded PSI	6.8.0	6.9.0
Dec 2005	CT#30	CP-050611	222	2	Removal of overhead in Private Identities handling in RTR	6.8.0	6.9.0
Dec 2005	CT#30	CP-050605	229	2	Use-Data description corrections	6.8.0	6.9.0
Dec 2005	CT#30	CP-050605	232	2	S-CSCF assignment checking for notregistered state	6.8.0	6.9.0
Dec 2005	CT#30	CP-050605	236	4	RTR correction	6.8.0	6.9.0
Dec 2005	CT#30	CP-050605	238	1	PPR correction	6.8.0	6.9.0
Dec 2005	CT#30	CP-050611	239	1	Private User Id in RTR	6.8.0	6.9.0
Dec 2005	CT#30	CP-050611	246	1	Server capabilities associations with features	6.8.0	6.9.0
Dec 2005	CT#30				Rel-7 version was created because of ETSI TISPAN references.	6.9.0	7.0.0
Mar 2006	CT#31	CP-060084	0243	1	SPT for mobile orig unregistered	7.0.0	7.1.0
Mar 2006	CT#31	CP-060159	0247	2	Removal of the terms Mobile Originated and Mobile Terminated	7.0.0	7.1.0
Mar 2006	CT#31	CP-060154	0254	-	Alignment of Annex E with .xsd file	7.0.0	7.1.0
Mar 2006	CT#31	CP-060154	0256	-	Incorrect implementation of CR 0198	7.0.0	7.1.0
Mar 2006	CT#31	CP-060065	0260	2	Handling of unknown errors	7.0.0	7.1.0
Mar 2006	CT#31	CP-060154	0263	2	Private User ID in PPR and RTR	7.0.0	7.1.0
Mar 2006	CT#31	CP-060065	0269	-	Message flow correction	7.0.0	7.1.0
Mar 2006	CT#31	CP-060065	0274	-	Default public-id and PPR	7.0.0	7.1.0
Jun 2006	CT#32	CP-060302	0285	-	S-CSCF reselection removal	7.1.0	7.2.0
Jun 2006	CT#32	CP-060308	0290	3	Correction of the normative text in the table 6.7	7.1.0	7.2.0
Jun 2006	CT#32	CP-060308	0292	2	Using SiFC feature to define optional S-CSCF capabilities	7.1.0	7.2.0
Sep 2006	CT#33	CP-060308	0296	-	S-CSCF assignment correction	7.2.0	7.3.0

Sep 2006	CT#33	CP-060417	0299	-	Default Public User ID either SIP URI or tel URI	7.2.0	7.3.0
Sep 2006	CT#33	CP-060399	0304	1	Barring Indication for public user identity	7.2.0	7.3.0
Sep 2006	CT#33	CP-060417	0306	2	Deletion of description about Authentication-Data-Item	7.2.0	7.3.0
Sep 2006	CT#33	CP-060399	0313	1	Registration message flow correction	7.2.0	7.3.0
Sep 2006	CT#33	CP-060417	0314	4	AS originating requests on behalf of a user	7.2.0	7.3.0
Sep 2006	CT#33	CP-060416	0317	2	Allowing a Display Name to be associated with a Public Identity.	7.2.0	7.3.0
Sep 2006	CT#33	CP-060417	0320	-	Update of the Table 6.7 "Guidelines for S-CSCF Capabilities"	7.2.0	7.3.0
Dec 2006	CT#34	CP-060553	0325	1	SDP reference correction	7.3.0	7.4.0
Dec 2006	CT#34	CP-060566	0326	1	New message flow about AS originating session	7.3.0	7.4.0
Dec 2006	CT#34	CP-060566	0327	1	Correction of Private Identity description in SAR	7.3.0	7.4.0
Dec 2006	CT#34	CP-060566	0330	3	Correction of error code in SAA	7.3.0	7.4.0
Dec 2006	CT#34	CP-060566	0332	1	Clarification on use of Authentication pending flag	7.3.0	7.4.0
Dec 2006	CT#34	CP-060566	0336	3	Optimization of handling of Wildcarded PSIs	7.3.0	7.4.0
Dec 2006	CT#34	CP-060555	0338	1	Wildcarded PSI as key in PPR	7.3.0	7.4.0
Dec 2006	CT#34	CP-060553	0342	1	Correction of the HSS behaviour in UAR/UAA command pair	7.3.0	7.4.0
Dec 2006	CT#34	CP-060735	0343	3	Clarification regarding URI canonicalization – 29.228	7.3.0	7.4.0
Mar 2007	CT#35	CP-070020	0346	3	Clarification of the server name in LIA	7.4.0	7.5.0
Mar 2007	CT#35	CP-070020	0350	3	User profile data synchronisation	7.4.0	7.5.0
Mar 2007	CT#35	CP-070020	0352	-	SAA result code correction	7.4.0	7.5.0
Mar 2007	CT#35	CP-070019	0353	2	Removal of roaming restrictions for Emergency Registrations	7.4.0	7.5.0
Mar 2007	CT#35	CP-070020	0354	-	Definition and use of the Wildcarded PSI information element	7.4.0	7.5.0
Jun 2007	CT#36	CP-070309	0358	1	Removal of editor's note on IMS Recovery Procedures	7.5.0	7.6.0
Jun 2007	CT#36	CP-070479	0359	2	Impacts of the IMS Communication Service Identifier	7.5.0	7.6.0
Jun 2007	CT#36	CP-070309	0361	2	Clarification on LIA	7.5.0	7.6.0
Jun 2007	CT#36	CP-070309	0365	1	Adding User-Authorization-Type is absent condition to UAR Detailed behaviour	7.5.0	7.6.0
Jun 2007	CT#36	CP-070312	0367	-	Modification to the tag RegistrationtType to RegistrationType in the Annex E	7.5.0	7.6.0
Sep 2007	CT#37	CP-070520	0374	1	Authentication failure and timeout handling	7.6.0	7.7.0
Sep 2007	CT#37	CP-070522	0378	-	Incorrect implemented CR 120r3	7.6.0	7.7.0
Sep 2007	CT#37	CP-070527	0379	-	User Data Already Available	7.6.0	7.7.0
Nov 2007	CT#38	CP-070743	0388	1	Handling of USER_UNKNOWN and NOT_SUPPORTED_USER_DATA error in PPA	7.7.0	7.8.0
Nov 2007	CT#38	CP-070744	0392	2	Alias	7.7.0	7.8.0
Nov 2007	CT#38	CP-070755	0376	6	Updates to 29.228 for Digest on the Cx Interface	7.8.0	8.0.0
Mar 2008	CT#39	CP-080019	0393	1	IMS Restoration after an S-CSCF failure	8.0.0	8.1.0
Mar 2008	CT#39	CP-080022	0395	2	Update for Supporting NASS-Bundled-Authentication	8.0.0	8.1.0
Mar 2008	CT#39	CP-080019	0398	-	SIP Digest password push	8.0.0	8.1.0
Mar 2008	CT#39	CP-080019	0400	1	Wildcarded Public User Identities	8.0.0	8.1.0
Jun 2008	CT#40	CP-080261	0399	3	Originating services after call forwarding	8.1.0	8.2.0
Jun 2008	CT#40	CP-080261	0406		XML example	8.1.0	8.2.0
Jun 2008	CT#40	CP-080267	0408		Emergency Registration for REGISTRATION_AND_CAPABILITIES	8.1.0	8.2.0
Jun 2008	CT#40	CP-080267	0410		Removal of restriction for barred user at Emergency Registrations	8.1.0	8.2.0
Sep 2008	CT#41	CP-080456	0413	2	Emergency Public User Identity removal	8.2.0	8.3.0
Sep 2008	CT#41	CP-080460	0420	1	Support of "Loose-Route" indication from HSS	8.2.0	8.3.0
Sep 2008	CT#41	CP-080463	0421		Cx Impacts of IMS Restoration Procedures	8.2.0	8.3.0
Sep 2008	CT#41	CP-080460	0423	2	Filter Criteria enhancement for 3rd party REGISTER	8.2.0	8.3.0
Sep 2008	CT#41	CP-080463	0425	1	Addition of Registered Private Identities in SAA	8.2.0	8.3.0
Sep 2008	CT#41	CP-080460	0426	1	Add Assigned S-CSCF name to SAA	8.2.0	8.3.0
Dec 2008	CT#42	CP-080698	0427	2	Service Restoration for Registered IMPU	8.3.0	8.4.0
Dec 2008	CT#42	CP-080707	0431	2	Support for IMS Service Level Trace	8.3.0	8.4.0
Dec 2008	CT#42	CP-080708	0432		Removal of Digest Domain	8.3.0	8.4.0
Dec 2008	CT#42	CP-080696	0433	3	Diameter Proxy Agent - an alternative User Identity to HSS resolution mechanism	8.3.0	8.4.0
Dec 2008	CT#42	CP-080708	0434	2	S-CSCF and AS procedures with Enhanced Filter Criteria	8.3.0	8.4.0
Mar 2009	CT#43	CP-090023	0435	1	Priority Service	8.4.0	8.5.0
Mar 2009	CT#43	CP-090026	0436	1	Multiple Registrations in Registration	8.4.0	8.5.0
Mar 2009	CT#43	CP-090036	0440	2	HSS Addresses	8.4.0	8.5.0
Mar 2009	CT#43	CP-090025	0441	1	Loose Route Indication	8.4.0	8.5.0
Mar 2009	CT#43	CP-090028	0442	2	Support for GPRS IMS Bundled Authentication (GIBA) in Cx	8.4.0	8.5.0
Sep 2009	CT#45	CP-090728	0447	1	Incorrect CR implementation	8.5.0	8.6.0
Dec 2009	CT#46		0452	1	Unregistered user clarification	8.6.0	8.7.0
Dec 2009	CT#46		0456	2	Session-Priority AVP	8.6.0	8.7.0
Dec 2009	CT#46		0457	2	HSS behaviour after PPA with unknown user	8.6.0	8.7.0
Dec 2009	CT#46		0458	1	Check of the S-CSCF Name	8.6.0	8.7.0
Dec 2009	CT#46		0460		IMPI must be sent in SAR for UE initiated requests	8.6.0	8.7.0
Dec 2009	CT#46				Upgraded unchanged from Rel-8	8.7.0	9.0.0
Mar 2010	CT#47	CP-100033	0462		Default IMPU	9.0.0	9.1.0
Mar 2010	CT#47	CP-100031	0468	1	Wildcarded Public Identity	9.0.0	9.1.0
Mar 2010	CT#47	CP-100033	0470	1	Priority service attribute	9.0.0	9.1.0
Mar 2010	CT#47	CP-100033	0474	1	User-Auth-Type not checked	9.0.0	9.1.0
Mar 2010	CT#47	CP-100033	0476	1	GIBA is not allowed when auth. Scheme is Unknown	9.0.0	9.1.0

Mar 2010	CT#47	CP-100042	0477	2	Clarification on the use of User-Data-Already-Available	9.0.0	9.1.0
Mar 2010	CT#47	CP-100015	0482		Server Capabilities	9.0.0	9.1.0
Mar 2010	CT#47	CP-100031	0466		RTR for wildcarded public user identity	9.0.0	9.1.0
May 2010					Xml-file corrected	9.1.0	9.1.1
Jun 2010	CT#48	CP-100412	0484	3	Table not aligned with XML schema for wildcarded identities	9.1.1	9.2.0
Jun 2010	CT#48	CP-100412	0487	3	SAR with NO_ASSIGNMENT correction	9.1.1	9.2.0
Jun 2010	CT#48	CP-100412	0489	2	Update of IETF Reference	9.1.1	9.2.0
Sep 2010	CT#49	CP-100447	0493	2	Wildcarded Identities handling	9.2.0	9.3.0
Sep 2010	CT#49	CP-100447	0495		Wrong order in table for XML schema	9.2.0	9.3.0
Sep 2010	CT#49	CP-100447	0497	2	Cx-MAR handling correction in restoration procedures	9.2.0	9.3.0
Sep 2010	CT#49	CP-100447	500	1	Ambiguity of Presence Conditions of IEs and AVP ABNF	9.2.0	9.3.0
Sep 2010	CT#49	CP-100447	507		Correction for de-registration procedure at restoration	9.2.0	9.3.0
Sep 2010	CT#49	CP-100447	504	2	Mandatory and optional capabilities handling	9.2.0	9.3.0
Dec 2010	CT#50	CP-100668	0519		Coding of SIP-Authorization AVP and SIP-Authenticate AVP	9.3.0	9.4.0
Mar 2011	CT#51	CP-110044	0522		Originating_CDIV Session Case including in XML	9.4.0	9.5.0
Jun 2011	CT#52	CP-110349	0528	2	Handling of RTR for Emergency Registration	9.5.0	9.6.0
Jun 2011	CT#52	CP-110356	0531	1	Emergency Restoration	9.5.0	9.6.0
Jun 2011	CT#52	CP-110356	0534		Incorrect Use of Result-Code AVP	9.5.0	9.6.0
Jun 2011	CT#52	CP-110356	0537	1	Error in assignment type for backward compatibility scenarios	9.5.0	9.6.0

History

Document history		
V9.0.0	January 2010	Publication
V9.1.0	April 2010	Publication
V9.1.1	June 2010	Publication
V9.2.0	June 2010	Publication
V9.3.0	October 2010	Publication
V9.4.0	January 2011	Publication
V9.5.0	April 2011	Publication
V9.6.0	June 2011	Publication